GÖTEBORGS UNIVERSITET

.

Betalningsmedel & dess risker

En studie om hur människor upplever risker vid användning av betalningsmedel

Means of payment and its risks

A study about how people perceive risks when using different means of payment

PHILIP ROBINSON
CHRISTOFFER ANDERSSON

Kandidatuppsats i informatik

Rapport nr. 2013:030
ISSN: 1651-4769

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2013

Abstrakt

Det finns idag många olika sätt att utföra betalningar på. Man kan bland annat använda sig av kontanter, bankkort, internet och även sin mobil när man handlar. Samtidigt ser vi idag att det dyker upp en del nya typer av tekniska betalningslösningar, så som till exempel Near Field Communication (NFC), mobilbank eller med hjälp av QR-koder. Eftersom att vi idag har relativt många sätt att betala på är det intressant att se vilket eller vilka betalningsmedel som människor främst föredrar. Användningen av olika betalningsmedel är inte helt riskfritt. Risker som till exempel skimming och nätfiske har fått mycket uppmärksamhet i media på senare tid, där det har skrivits om människor som blivit bestulna på sina kortuppgifter och blivit av med sina pengar. Därför har vi valt att undersöka vilka risker man upplever vid användning och hantering av olika betalningsmedel, samt vilket eller vilka betalningsmedel som främst föredras. För att ta reda på detta har vi utformat en enkätundersökning för att se hur människor ställer sig till dessa frågor. Det vi har funnit är att kontokort är det betalningsmedel som majoriteten föredrar, medan endast 5 % föredrar att använda mobilen. Detta tror vi kan bero på att det fortfarande är väldigt nytt i Sverige vilket vi kan se från vår enkätundersökning, där 32 % någon gång använt sin mobil för att betala. Däremot så kan vi se att 44 % av respondenterna kan tänka sig att använd sin mobil som ett betalningsmedel i framtiden. Detta tyder på att det förmodligen kommer bli allt vanligare i framtiden med denna typ av betalning.

Det vi har sett är att det finns många olika risker som upplevs vid de olika betalningsmedlen. Resultatet visar att det kan vara situationen som spelar roll, eller hur van man är vid till exempel användning av tekniken. Men också att åldern verkar ha en betydelse till hur man uppfattar risker. Riskerna som vi har hittat har vi valt att kategorisera enligt följande för att på så sätt lättare få en överblick över dem. Dessa kategorier är: fysisk hantering, informationshantering, skadlig programvara, oseriösa aktörer och tekniska problem.

Nyckelord: Betalningsmedel, kontanter, kontokort, internetbetalning, mobilbetalning, risker.

Abstract

Today you can pay in many different ways. You can for instance use cash, credit cards, internet and now even with your mobile phone. Today we can also see new types of technical payment solutions being developed, such as Near Field Communication (NFC), mobile banking or through the use of QR-codes. We have today many different payment methods; therefore it's interesting to see which payment method people prefer the most. The use of different means of payment is not entirely risk free. Risks such as skimming and phishing have lately received much attention in the media, where you can read about people who had their credit card information stolen and lost their money. Therefore, we have chosen to study what kind of risks people experience in the use of the different payment methods, and which method they prefer to use. To find this out, we have created a survey that helps us to see how people think around these questions. From the survey we found that the majority preferred credit card, while only 5% preferred to use their mobile phone to make payments with. We believe that this may be because mobile payment still is very new in Sweden, which we also can see from our survey, where 32% of the respondents answered that they had tried it. However, in our survey we can see that 44% of all the respondents are willing to use their mobile phones as a payment method in the future. This indicates that this kind of payment method probably will be more common in the future.

What we also have seen from our survey is that there are many different types of risks among the various payment methods. Where the situation sometimes is a factor, or how technical experienced the user is. But we also found that the age seems to have a significant role in how they perceive risks. To make it easier to get an overview of the risks that we have found, we categorized them in the following categories: physical management, information management, malware, rogue actors and technical problems.

Keywords: Means of payment, cash, Credit card, internet payment, mobile payment, risks.

TACK

Vi vill tacka Agneta Ranerup som har varit vår handledare genom arbetets gång och hjälpt oss med att ge feedback och förslag.

Vi vill även passa på och tacka alla som har deltagit och svarat på vår enkätundersökning.

Innehåll

1. Inledning 6
1.1 Syfte & frågeställning 7
1.2 Disposition 7
2. Beskrivning av betalningsmedel 9
2.1 Kontanter 9
2.2 Kortbetalning 9
2.3 Internetbetalning 10
2.4 Mobilbetalning 11
3. Teori 13
3.1 Risker vid kontantbetalning 13
3.2 Risker vid kortbetalning 13
3.3 Risker vid internetbetalning 14
3.3.1 Datorvirus 15
3.4 Risker vid mobilbetalning 16
3.5 Sammanfattning och kategorisering av risker 17
3.6 Teorins roll i studien 18
4. Metod 19
4.1 Enkäter 19
4.2 Urval & spridning 19
4.3 Metod för att analysera data 20
4.4 Validitet & Reliabilitet 20
5. Resultat 22
5.1 Betalningsmedel som används och varför 22
5.2 Upplevda risker 26
6. Diskussion & slutsats 33
6.1 Resultatdiskussion 33
6.2 Slutsats 37
6.3 Vidare forskning 37
Referenser 38

Bilaga 1 – Enkät
Bilaga 2a – Öppna svar: risker
Bilaga 2b – Öppna svar: medias påverkan

1. Inledning

Det finns idag många olika sätt att utföra betalningar på. Man kan bland annat använda sig av kontanter, bankkort, internet och även sin mobil när man handlar. Mobilbetalning är dock något ganska nytt i Sverige och har inte riktigt etablerats helt än. Samtidigt dyker det upp en del nya typer av tekniska betalningslösningar, som till exempel där man kan använda sig av Near Field Communication (NFC) för att snabbt och enkelt kunna utföra betalningar med. NFC är samma typ av teknik som används vid till exempel stämpling av busskort eller liftkort i skidliften (Ondrus & Pigneur, 2009). Som man kan se finns det idag ett par redan etablerade betalningsmedel och även ett par som idag håller på att etablera sig, framförallt kanske då att kunna använda sin smartphone som ett betalningsmedel. Det har tidigare gjorts försök med att införa nya betalningsmedel, som till exempel cashkortet som infördes 1997. Cashkortet var en teknisk lösning där ett plastkort laddades med pengar vid en särskild terminal. Men det etablerades aldrig på grund av att det var dyrt och att kreditkorten började slå igenom (Ivarsson, 2010). Detta kan idag liknas vid mobilbetalning som också är ett försök att etablera ett nytt betalningsmedel. Därför är det intressant att se hur mobilbetalning kommer att utvecklas framöver, om det kommer bli det nästa stora betalningsmedel eller om det kommer att misslyckas som cashkortet gjorde.

Eftersom att vi idag har relativt många sätt att betala på kan det vara intressant att se vilket eller vilka betalningsmedel som människor främst föredrar. Är det fortfarande vanligare med kontanter, eftersom det kanske för många är lättare att ha koll på hur mycket man spenderar. Eller börjar man nu tröttna på att hantera kontanter som nu istället leder till att kortbetalningen börjar ta över allt mer och mer? Och hur står sig intresset för de nyare sätten att betala som nu börjar införas jämfört med de redan etablerade betalningsmedlen? Drar sig den yngre generationen åt de mer tekniska lösningarna, som att betala via internet, via smartphones o.s.v. som gör att dessa kommer bli mer populära i framtiden?

I samband med att det kommer nya betalningsmedel, men som också gäller de redan etablerade betalningsmedlen, är att det alltid finns risker vid hantering och användning av dessa. Ett exempel är att det kanske upplevs som en större risk att bli rånad på kontanter om man har en stor summa pengar på sig. Eller att det har uppstått ett datorhaveri i en butik, vilket gör att du inte kan använda ditt kort när du ska betala och därför måste använda dig av något annat betalningsmedel. Risker som skimming och nätfiske har nyligen även fått mycket uppmärksamhet i media, där det har skrivits om människor som har blivit bestulna på sina kortuppgifter och blivit av med sina pengar (GP, 2012). Det finns risker med alla typer av betalningsmedel och med tanke på den stora uppmärksamheten detta ämne har fått i media, så är det intressant att undersöka hur människor ser och tänker kring detta. Upplever människor risker med de olika betalningsmedlen och om det i så fall görs avvägningar för

vilka betalningsmedel man använder eller kanske undviker. Eller om man helt enkelt bara använder olika betalningsmedel utan att tänka på de risker som kan finnas.

1.1 Syfte & frågeställning

Syftet med studien är att med en kvantitativ enkätundersökning studera människors val av betalningsmedel, och vad som kan vara de bidragande faktorer till varför de använder ett specifikt sätt att betala på. De betalningsmedel som vi tar upp i studien är kontanter, kontokort, internetbetalning och mobilbetalning. Anledningen till varför vi valt just dessa fyra är för att vi anser att dem är några av de vanligaste och mest utbredda betalningsmedlen idag. Den grupp vi har tänkt fokusera på är konsumenter, d.v.s. de som använder betalningsmedel i sitt vardagsliv för att handla med. Anledningen till varför det är intressant att se vad människor föredrar, är bland annat för att se om utvecklingen av betalningsmedel går i samma riktning som allmänhetens uppfattning. Tekniken idag är en stor del av människors liv och det utvecklas ständigt nya tekniska lösningar, som till exempel att göra det möjligt för konsumenter att betala med sina smartphones i butiker. Situationen kan även påverka varför ett betalningsmedel används framför ett annat, då det till exempel kan vara så att det endast accepteras kort eller kontanter i butiken. En annan del av studien är att vi undersöker hur människor upplever risker vid betalningsmedel. Avsikten är bland annat att se om det kan påverka vilka betalningsmedel som föredras att använda.

Att det finns risker med olika betalningsmedel kan nog de flesta enas om, men vilka är det som man verkligen upplever som risker? Med detta menar vi de risker som individen upplever vid användningen av ett specifikt betalningsmedel, där det är vissa risker som man upplever ha större chans att inträffa än andra. Tanken med studien är inte att gå igenom och ta upp alla möjliga risker som kan finnas vid de olika betalningsmedlen, utan att istället begränsa oss till de risker som har uppmärksammats mycket i media på senare tid. Vi kompletterar även detta med några risker som vi själva anser är relevanta att ta upp i studien.

Utifrån detta har vi formulerat vår frågeställning på följande sätt:

Vilka betalningsmedel föredrar människor, samt vilka risker upplever man vid hantering och användning av dem?

1.2 Disposition

Vi kommer först i avsnitt 2 att presentera och beskriva de olika betalningsmedel som ingår i studien, vilka är kontanter, kontokort, internetbetalning och mobilbetalning. Vi börjar med att förklara varför vi har valt just dessa fyra betalningsmedel, för att sedan gå vidare med att beskriva dem en efter en. Avsnitt 3 innefattar vår teoretiska referensram där vi först motiverar valet av de risker som vi valt att ta upp, för att sedan gå igenom risker kring varje betalningsmedel. Teorin ligger som grund för hur vi har utformat vår enkät. I avsnitt 4

beskriver vi vår datainsamlingsmetod, hur urvalet av undersökningens deltagare har gjorts och hur vi har valt att sprida enkäten. Samt att vi beskriver hur vi har analyserat vår insamlade data. I avsnitt 5 presenteras resultatet av vår studie, vilket görs i form av diagram med tillhörande beskrivningar. Slutligen i avsnitt 6 för vi en diskussion kring det vi har fått fram i studien. Vi avslutar med en slutsats och ger förslag på fortsatt forskning.

2. Beskrivning av betalningsmedel

Vi kommer här att gå igenom och beskriva de olika betalningsmedlen som undersöks i vår studie. Dessa är kontanter, kortbetalning, internetbetalning och mobilbetalning. Anledningen till varför vi valt just dessa fyra är för att vi anser att dem är de vanligaste och mest utbredda betalningsmedlen idag. Ett undantag är möjligen mobilbetalning, men vi valde även att inkludera detta eftersom smartphones är så pass vanligt idag och att det nu ständigt utvecklas tjänster som gör det möjligt att betala med mobilen i till exempel butiker och liknande. Ett område där man redan idag kan se detta tydligt är bland olika tjänster för smartphones, som till exempel App Store, Google play och Itunes. I dessa tjänster är det möjligt att köpa appar, film, musik o.s.v. direkt via telefonen, vilket idag är väldigt vanligt (Dediu, 2013).

2.1 Kontanter

Kontanter är ett samlingsnamn för sedlar och mynt som idag kan ses som ett traditionellt sätt att betala, där betalningen sker mellan två personer, köpare och säljare. Detta betalningsmedel är det enda som inte kräver någon mellanhand vid just köptillfället, så som diverse olika system. Utan det är bara köparen och säljaren som är involverade vid överföringstillfället av pengarna. Detta betalningsmedel är också bland det vanligaste sättet att betala när två privatpersoner träffas för att köpa eller sälja eftersom det är ett snabbt och smidigt sätt att betala på. Kontantbetalning karaktäriseras ofta med att leveransen av varan eller tjänsten sker i samband med att betalningen görs och att man direkt får tillgång till det man köpt. Till skillnad från om man skulle köpa något över internet, där man betalar för varan men får vanligtvis inte tillgång till den förens inom några dagar.

2.2 Kortbetalning

Kortbetalning är ett nyare sätt där man istället för kontanter använder ett plastkort som är kopplat till innehavarens bankkonto. För att läsa av kortet används antingen en magnetremsa eller ett chip som kopplar kortet till ett specifikt bankkonto. Magnetremsan består av en svart tunn filmremsa som lagrar 1:or och 0:or som översätts till ett unikt nummer när den dras genom en kortläsare. Det unika numret är i sin tur kopplat till ett bankkonto som pengarna dras ifrån. Magnetremsan anses oftast som osäkert eftersom informationen på den enkelt kan kopieras och förfalskas. För att förhindra detta består många av dagens plastkort av ett chip, vilket är mycket säkrare att använda eftersom informationen på chippet inte kan kopieras på samma sätt som vid magnetremsan (Kreditkortinformation, utan årtal).

För många är kortbetalning ett självklart val då det är smidigt och enkelt att använda, där du antingen ger en namnsignatur på ett kvitto eller att du skriver in en PIN-kod för att godkänna

köpet. Men också att man slipper gå runt med kontanter i plånboken och oroa sig för att bli bestulen på sina pengar eller att man tappar dem. Till skillnad från ett kort där du enkelt spärra dina uppgifter om du skulle bli av med kortet och på så sätt förhindra att pengarna blir stulna.

Vid kontantbetalning är det bara köparen och säljaren som är inblandade i transaktionen jämfört med kortbetalning där det krävs att flera parter är involverade: köparen, säljaren, deras banker och kortföretaget. Detta resulterar i en mindre transaktionsavgift för handlare, vilket har lett till att mindre butiker som säljer många billiga varor (godis eller liknande) istället kan gå med förlust på grund av denna transaktionsavgift som dras vid varje transaktion. På grund av detta tar en del mindre butiker inte längre emot kortbetalning för mindre summor och kunden tvingas därmed i dessa fall att betala med kontanter.

2.3 Internetbetalning

Att handla över internet har blivit allt mer vanligare (Findahl, 2012), då det i många fall kan vara billigare att handla på nätet än att göra det i en fysisk butik. Samtidigt kan internet även användas som en informationskälla för att jämföra priser, läsa recensioner o.s.v. om den varan som man tänkt köpa. Att handla på internet kan även upplevas som väldigt bekvämt eftersom du nästan kan befinna dig var som helst när du utför dina köp (Svensk Handel, 2011).

Det finns många olika sätt att utföra betalningar på internet, vilka kan se olika ut beroende på sammanhanget som betalningen görs i och de betalningsalternativ som erbjuds vid köptillfället. Till exempel i kassan på en nätbutik får kunden välja på vilket sätt hon vill betala varan eller tjänsten på. Ett av dessa kan vara att direkt betala med hjälp av sitt kontokort genom att skriva in sina kortuppgifter. Ett annat sätt att betala är med hjälp av en faktura som skickas hem till kunden. Betalningen av fakturan kan ske via sin internetbank genom att skriva in OCR-numret som står på fakturan och sedan verifiera köpet. Verifieringen av köpet kan se ut på olika sätt beroende på vilken internetbank som används, men sker oftast med hjälp av en bankdosa och en kod. Det går även att använda direktbetalning som direkt skickar kunden vidare till sin internetbank, där kunden sedan loggar in och väljer vilket konto transaktionen ska ske ifrån. Fördelen med direktbetalning är att kunden aldrig behöver ge ut kortuppgifter vid sitt köp.

Det sker en ständig utveckling av tjänster för att göra det smidigare och säkrare för konsumenter att betala över internet. Ett exempel på en sådan tjänst är PayPal där användare kan registrera sig och säkert spara sina kortuppgifter. När användaren sedan ska betala för något online erbjuds ibland möjligheten till att betala med hjälp av PayPal. Detta går till genom att användaren helt enkelt loggar in med sina PayPal-uppgifter, bekräftar och betalar. Eftersom allt är sparat i PayPal behövs inte kortuppgifter lämnas ut inför varje köp

på olika nätbutiker. Med PayPal kan även betalningar mellan två privatpersoner göras på ett smidigt och säkert sätt. Varje PayPal-konto är kopplat till en mailadress och det räcker att endast ange sin mailadress för att göra en överföring, vilket innebär att inga kortuppgifter behövs ge ut (Paypal, utan årtal).

Ett annat exempel på detta är MasterPass som är en ny kommande tjänst från Mastercard. Masterpass är en digitalplånbokservice som sparar betalnings- och leveransinformation på en säker plats. Den fungerar på så sätt att när man har fyllt sin varukorg och skall betala klickar man på "Handla med MasterPass" och väljer sin plånbok. Där du antingen direkt loggar in på sidan, eller att du skickas vidare till MasterCard för att slutföra ditt köp. När du är inloggad kan du välja mellan dina sparade betalkort och postadresser eller att du väljer att skriva in nya uppgifter och sen slutföra ditt köp. Fördelen med MasterPass är att man enbart behöver komma ihåg sina inloggningsuppgifter till MasterPass, istället för att behöva skriva in nya uppgifter varje gång man gör ett nytt köp på en hemsida (Mastercard, utan årtal). Tjänster som dessa kommer vi förmodligen att se allt mer av, då näthandeln blir allt mer vanligare och ständigt växer, vilket därmed även ställer större krav på användarvänligheten och säkerheten.

2.4 Mobilbetalning

Mobilbetalning är idag inte speciellt utbrett i Sverige ännu. Bara ett fåtal butiker har det som alternativ för att testa på det och se hur det fungerar. Men det förväntas att bli allt mer vanligt då nya tjänster ständigt utvecklas och testas. Då bland annat de stora operatörerna Telia, Tele2, Telenor och 3 gått ihop och startat ett nytt gemensamt bolag för just mobilbetalning, vilket är vad detta bolag endast kommer att fokusera på. Detta för att dels hjälpa till med att sätta fart på utvecklingen och öka implementeringen utav mobila betalningstjänster, men dels för att se till så att kunder i framtiden slipper skriva på avtal för varje operatör (Lindström, 2011). Det utvecklas bland annat tjänster som kommer göra det möjligt att betala i butiker med hjälp av NFC, som fungerar genom att mobilen innehåller ett chip som fungerar som en radiosändare (Telenor, 2012). Det enda som behövs är att hålla mobilen nära en betalningsterminal för att enkelt och snabbt betala, likt hur ett busskort stämplas. Även Swedbank släpper redan i år sin egen mobilbetalningstjänst "Bart", vilket är en applikation som kan användas när du handlar i butiker. Den fungerar genom att en QR-kod läses av med hjälp av applikationen i sin telefon. En QR-kod är en form av streckkod som fås i kassan där kunden läser av den med hjälp av applikationen och sedan godkänner köpet (Swedbank, utan årtal(a)).

Det vi kan se idag är att banker börjar utveckla tjänster som gör det möjligt att använda sin smartphone för att utföra bankärenden. Mobilbank fungerar likt internetbank, men istället för att använda sig av en dator går det nu att använda sin smartphone. Där det enkelt går att få en ekonomisk överblick, göra betalningar och överförningar (Swedbank, utan årtal(b)).

Ett område inom mobilbetalning som redan idag är utbrett, är försäljning av appar, musik, film o.s.v. (Dediu, 2013). Ett tecken på att detta blir allt vanligare är att antalet nerladdade appar i App Store har ökat med 30 miljarder mellan 2011 och 2013 (Apple, 2011, 2013). Försäljningen sker oftast via tjänster som App Store, Google play och Itunes direkt i mobilen. För att köpa applikationer, film, musik och annat i dessa tjänster behövs ett konto som innehåller användarens kortuppgifter. Efter ett godkännande dras pengar direkt från det angivna kontot och den köpta varan blir sedan tillgänglig på användarens smartphone.

Att betala med sin mobil blir allt mer populärt, vilket visade sig redan i slutet av 2011 då Telia presenterade en undersökning gällande intresset av mobilbetalning. I undersökningen visade det sig att 30 procent av de tillfrågade svarar att dem redan idag (2011) skulle vilja använda sina telefoner för att utföra betalningar. 50 procent säger att de räknar med att göra det inom högst 2 år. Undersökningen visar även att många ser mobilbetalning som ett naturligt nästa steg i utvecklingen av smartphones och betalningsmedel (Zirn, 2011).

3. Teori

När det handlar om betalningar, så är säkerheten något som är extremt viktigt. I detta avsnitt kommer vi därför att gå igenom olika typer av risker som kan finnas vid de olika betalningsmedlen som vi tidigare har presenterat. Tanken här är inte att gå igenom alla möjliga risker som kan finnas vid olika typer av betalningar, utan vi har till största del begränsat oss till de risker som vid senare tid uppmärksammats i media. Vi kompletterar även detta genom att ta upp några risker som vi själva anser vara relevanta. Vi går stegvis igenom respektive betalningsmedel för sig och tar upp de risker som finns för dessa. Slutligen ges en kategoriserad sammanfattning av alla de risker som vi tagit upp för att lättare kunna urskilja och diskutera dem.

3.1 Risker vid kontantbetalning

När det gäller risker kring kontantbetalning är det risker som handlar mer om innehavandet och hantering av kontanterna. En risk med att ha pengar kontant är att bli rånad eller att bli av med dem på andra sätt (Svenska Bankföreningen, 2010). Där mängden av kontanter har en bidragande faktor till hur stor risk som upplevs vid innehavandet av kontanter. Ett exempel är att det kan upplevas som en större risk att bära på 10 000 kr till skillnad från 50 kr, eftersom det rör sig om en större mängd pengar. Nackdelen med kontanter är också att det är svårt att få tillbaka pengarna då det inte går att spåra dem på samma sätt som de elektroniska betalningsmedlen. Eftersom elektroniska betalningsmedel lämnar spår i det finansiella systemet är det möjligt att se vad för transaktioner som gjorts och till vilka konton pengarna har förflyttas mellan. Detta gör det lättare att ta reda på vart pengarna har tagit vägen (Svenska Bankföreningen, 2010).

Jämfört med många andra betalningsmedel är kontanter ett fysiskt medel och därmed finns det inte lika många tekniska risker. Det finns istället risker som handlar mer om hantering och liknande av kontanter.

3.2 Risker vid kortbetalning

Kortbetalning är ett betalningsmedel som många i Sverige använder, det finns dock en del risker med denna typ av betalning. I media har man på senare tid kunnat läsa mycket om att man bland annat ska vara uppmärksam över de kortmaskiner och uttagningsautomater som du använder när du ska betala eller ta ut pengar. Då flera har blivit utsatta av så kallat “skimming”, där de har blivit bestulna på sina kortuppgifter. Exempel på detta är en artikel från GP, där de skriver om att många som har använt sig av en biljettautomat i Uppsala kan ha drabbats av skimming. Polisen slog larm efter att en privatperson rapporterat om att det var något som satt löst på biljettautomaten, vilket senare visade sig att handla om skimmingutrustning (GP, 2012). Skimming är en bedrägerimetod som går ut på att

elektroniskt kopiera någon annans kortuppgifter, vilket vanligtvis görs genom att magnetremsan på kortet läses av. Sedan för man över den drabbades kortuppgifter till ett annat falskt kort utan att den drabbade vet om det. Det är svårt i stunden att inse att ens kort har blivit kopierat. Detta brukar man först märka då man börjar få hem konstiga räkningar, eller inser att det fattas pengar på sitt konto. Skimmingutrustning kan monteras på bankomater, där en avläsare installeras vid kortintaget som läser av dina kortuppgifter när du stoppar in ditt kort. Samtidigt kan även utrustning som kameror installeras ovanför som ett sätt att kunna läsa av och spela in din PIN-kod när du skriver in den (Patidar & Sharma, 2011).

Vidare finns det även andra sätt att bli drabbad av kortbedrägeri, där ens kortuppgifter på olika sätt hamnar i fel händer. För ett tag sedan gick polisen ut med en varning, då en taxichaufför i tjänst lurat till sig kortuppgifter när människor betalat sin taxiresa med kort. Genom att chauffören inte ändrat standardinställningarna på kortmaskinen, skrev den ut hela kortnumret på kvittot, som chauffören sedan sparat. Med hjälp av detta kunde sedan samma transaktion genomföras igen vid flera olika tillfällen. Eftersom summorna är såpass små och att transaktionerna utfördes periodvis med längre mellanrum, är det lätt att den drabbade inte lägger märke till dem (Eriksson, 2012).

En annan typ av risk inom kortbetalning är att bli av med kortet, till exempel genom att tappa det eller bli bestulen på det. Skulle detta inträffa finns risken att någon får åtkomst till alla de pengar som finns tillgängliga på det bankkonto som kortet är kopplat till. Slutligen finns det även en risk att handlaren skriver in fel belopp när man ska betala med sitt kort. Speciellt om man inte är uppmärksam över summan som skrivs in, eller om man inte kollar på sitt kvitto. I en artikel från norska tv2 skriver man om detta, där man förklarar hur en person fick betala 85 000 norska kronor för en kebab efter att man i kassan av misstag angett fel belopp. Dock fick den utsatta i detta fall tillbaka sina pengar efter att felet senare uppmärksammats (Lygre, 2013).

3.3 Risker vid internetbetalning

En av de största riskerna när det kommer till internetbetalning är rädslan hos människor när de behöver lämna ut sina kortuppgifter, mailadresser osv. Man är rädd för att lämna ut känslig information eftersom att man inte riktigt vet hur information hanteras och hur säkra ens uppgifter är hos olika företag (Cho et al. 2006).

En annan risk som finns med betalning på internet är nätfiske, vilket är en metod som blir allt vanligare (Weider et al. 2008). Nätfiske är ett sätt att stjäla personlig information som användarnamn, lösenord och kortuppgifter. Detta går till genom att det skickas mail som ser ut att komma från till exempel en bank eller andra finansiella institutioner. Det kan exempelvis stå att deras databaser har kraschat och vill därför att man fyller i sina uppgifter

igen för att de skall kunna åtgärda felet. I mailet ges sedan en länk till en hemsida som ser identisk ut med bankens hemsida, där de vill att man skall fylla i sina uppgifter, men i själva verket är det en bluffhemsida som enbart är till för att komma åt kortuppgifter. Ett annat liknande sätt kan gå till genom att det skickas mail som påstår att du har vunnit ett pris och enbart behöver fylla i dina uppgifter för att få priset, men egentligen är även detta ett försök till att få tag på känsliga uppgifter (Patidar & Sharma, 2011).

En annan risk som finns när du handlar på internet, är oseriösa nätbutiker. Detta kan handla om att butiken inte levererar de varor som kunden har beställt och redan betalat för. Ett exempel på detta är Kameraexperten.se som under en längre tid hade skapat sig ett bra rykte genom att sköta affärerna korrekt. Detta var dock bara en strategi av kameraexperten för att sedan vid julhandeln 2008 kunna locka till sig så många kunder som möjligt genom att ha extremt låga priser. De varor som kunderna hade beställt och betalat för levererades sedan aldrig, utan detta var bara en bluff av Kameraexperten för att kunna få in så mycket pengar som möjligt under julhandeln (Rådmark, 2009).

3.3.1 Datorvirus

En annan risk är att kriminella kan komma åt dina kortuppgifter och annan känslig information genom datorer och internet, med hjälp av olika typer av virus. Virus är en skadlig programkod eller datorprogram som installeras på din dator, oftast utan att det märks av. För att viruset skall kunna sprida sig infekterar den andra program och kopierar sig själv och fäster sig vid programmen. Vilket innebär att när programmet körs kan viruset sprida sig ännu mer och även utföra andra operationer som viruset är konstruerat att göra (Mishra & Ansari, 2012). Keyloggers och trojaner är två typer av virus som är konstruerade för att komma åt känslig information och förstöra på olika sätt för den utsatta.

En trojansk häst är ett virus som har fått namnet genom sagans trojanska häst, som var en stor ihålig trähäst där soldater gömde sig i. En trojansk häst inom virus fungerar på liknande sätt, det är ett program som utger sig var något bra för att på så sätt få användaren att installera eller köra programmet. När trojanen sedan är installerad, kan personen bakom trojanen få tillgång till den utsattes dator, vilket oftast inte märks av förens skadan redan är skedd. Genom att ha tillgång till datorn kan personen på så sätt stjäla känslig information som finns sparad och använda denna för att till exempel handla på nätet, eller göra bankärenden med. (Symantec, 2007)

Keyloggers var till en början utvecklade för att hjälpa till med legitim övervakning. Att med hjälp av keyloggers kunna övervaka till exempel ens anställda så att de inte gav ut känslig information, eller för föräldrar att övervaka sina barn när de är ute och surfar på internet. Problemet i dagsläget är att det nu även används för kriminella aktiviteter som går ut på att programmet läser av vilka knapptryckningar som görs. När den som är infekterad av en

keylogger skall logga in på sin bank eller göra ett köp via internet kan keyloggern registrera vilka knapptryckningar som görs. Sedan skickas informationen ut till hackaren, som då får tillgång till det som keyloggern har registrerat, vilket kan vara till exempel kortuppgifter, lösenord eller liknande. Installationen av en keylogger kan gå till på olika sätt, så som att en slutanvändare klickar på en bifogad fil som hackaren har skickat, därefter installerar den sig själv likt ett virus. Det kan också vara så att datorn redan är infekterad av en trojan, där trojanen har möjligheten att ladda ner andra skadliga program till datorn, som till exempel en keylogger. Eller att hackaren utnyttjar brister i webbläsaren, när en slutanvändare sedan surfar in på en infekterade hemsidan, kan keyloggern laddas ner utan att det märks (Heron, 2007).

För att hackaren skall kunna ta del av informationen som keyloggern har loggat behöver han skicka informationen till sig själv så att han får tillgång till den. Detta kan göras på flera olika sätt som till exempel att keyloggern krypterar datan och sedan skickar informationen via en chatt tjänst, eller att den skickar informationen till en hemsida. Det kan också ske genom att det skapas en peer-to-peer koppling mellan de infekterade datorerna och på så sätt kan informationen hämtas (Heron, 2007).

3.4 Risker vid mobilbetalning

Likt bankkort är många mobila betalningstjänster direkt kopplade till användarens kontokort. Om man skulle tappa sin mobil, eller om den skulle bli stulen, så riskerar man att någon får direkt tillgång till ens pengar (Metro, 2013). Mobilbetalning har också liknande risker som vid internetbetalning, där det är samma rädsla med att ge ut personliga uppgifter till olika mobilbetalningstjänster. Man är rädd för hur ens personliga information hanteras och man vet inte riktigt hur säker informationen är hos mobilbetalningsföretagen (Mallat, 2006). Eftersom smartphones kan liknas en liten dator som har ständig uppkoppling till internet, finns även här risk för skadliga applikationer. Dessa skadliga applikationer fungerar i princip på samma sätt som på en dator, där applikationer som installeras på sin smartphone kan likna helt vanliga spel eller program, men som i själva verket innehåller virus i form av trojaner och annan skadlig kod. En del av dessa trojaner fokuserar helt på att stjäla pengar från internetbanker, genom till exempel keyloggers som loggar lösenord och annan känslig information. Denna information skickas sedan vidare till hackaren som använder den för att ta ut pengar från den utsattes konto (Delac et al. 2011).

3.5 Sammanfattning och kategorisering av risker

För att få en bättre överblick på de risker som har presenterats i tidigare avsnitt har vi valt att göra en kort sammanfattning av dem i form av en tabell (se Tabell 1). Det vi kan se är att vissa av riskerna överlappar mellan de olika betalningsmedlen. Så som att "rånad" och "tappa" förekommer på flera ställen. Vi har även valt att dela in riskerna i kategorierna fysisk hantering, information hantering, skadlig programvara och oseriösa aktörer som kan ses i Tabell 2.

Kontanter
- *Rånad.* - *Tappa kontanterna.*
Kontokort
- *Rånad.* - *Tappa kontokortet.* - *Skimming.* - *Att fel summa skrivs in när du betalar.* - *Bli bestulen på kortuppgifter när du lämnar ifrån dig kortet (t.ex. när du betalar).*
Internetbetalning
- *Lämna ut personliga uppgifter.* - *Lämna ut kortuppgifter.* - *Phishing (nätfiske).* - *Oseriösa butiker på nätet.* - *Virus, trojaner, keyloggers etc.*
Mobilbetalning
- *Bestulen på mobilen (Som därmed kan ge tillgång till internetbank).* - *Tappa mobilen (Som därmed kan ge tillgång till internetbank).* - *Lämna ut personliga uppgifter.* - *Skadliga appar.*

Tabell 1. Sammanfattning av risker.

Kategorisering av risker:

Fysisk hantering
- *Bestulen på kontanter, kontokortet eller mobilen.* - *Tappa kontanter, kontokortet eller mobilen.* - *Skimming.*
Informationshantering
- *Lämna ut personliga uppgifter (internet och mobilbetalning).* - *Lämna ut kortuppgifter.* - *Phishing (nätfiske).* - *Fel summa skrivs in (i butik).*
Skadlig programvara
- *Virus, trojaner, keyloggers etc.* - *Skadliga appar.*
Oseriösa aktörer
- *Oseriösa butiker på nätet.* - *Bestulen på kortuppgifter när du lämnar ifrån dig kortet.*

Tabell 2. Kategorisering av risker.

I Tabell 2 visas en kategorisering av de risker som tagits fram, där fysisk hantering handlar om risker som har med själva hanteringen att göra. Så som till exempel att kontanter tappas eller blir bestulna, eller att bli utsatt för skimming när ett uttag från en bankomat görs. Informationshantering innefattar risker där känslig information lämnas ut på internet, då det finns en osäkerhet på hur informationen hanteras. Skadlig programvara är kategoriseringen av de risker som har att göra med program som installeras på datorn eller mobilen i syfte att stjäla känslig information. Den sista kategorin handlar om oseriösa aktörer, som till exempel att en nätbutik inte levererar de varor som utlovats.

3.6 Teorins roll i studien

Teorin har bidragit med förståelse för några av de mest uppmärksamma risker som finns kring de betalningsmedel vi tar upp i studien, vilket på så sätt har hjälpt oss att bygga vår enkät. Genom att förstå vilka risker och vad för problematik det finns kring dessa har vi kunnat se till så att enkäten har rätt fokus. Samtidigt som teorin har hjälpt oss att beskriva riskerna på ett förståeligt sätt i enkäten. Genom att respondenterna förstår vad frågorna innebär, underlättar det sedan för oss när vi skall analysera den data vi får tillbaka från enkätundersökningen. Slutligen tar vi även hjälp av teorin för att diskutera resultatet i diskussionsavsnittet.

4. Metod

I det här avsnittet kommer vi att behandla vår metod, där vi bland annat skriver om den datainsamlingsmetod vi har valt att använda och varför, samt hur vi kommer göra vårt urval av informanter. Eftersom vi vill studera vilka betalningsmedel människor föredrar, samt vilka risker de upplever vid hantering och användning av dem har vi valt att använda oss av enkäter. Detta eftersom vi vill kunna nå ut till en större publik för att på så sätt se vilka betalningsmedel som är de mest populära i Sverige. Fördelen med enkäter är att det underlättar för oss när vi jämför svaren mellan de olika informanterna. Samtidigt som vi kan få fram numeriska värden på svaren, vilka vi sedan kan använda för att dra slutsatser om hur olika grupper av människor ställer sig kring denna fråga.

4.1 Enkäter

Vi har valt att utforma vår enkät med en hög grad av standardisering och strukturering (Patel & Davidson, 2011). Detta innebär att enkäten består av fasta svarsalternativ, eller att man på en flergradig skala markerar det värdet som stämmer bäst överens med vad man tycker. Om testpersonen har ett eget svar som inte finns angivet på vår enkät lämnar vi i vissa fall utrymme för ett kommentarsfält där man kan fylla i sitt egna svar. Genom att utforma enkäterna på detta sätt, där de svarar på samma frågor och i samma ordning, underlättar det för oss när vi skall jämföra de olika svaren med varandra. För att utformningen av vår enkät ska bli så bra som möjligt har vi innan studerat relaterade studier och litteratur kring ämnet, för att på så sätt se till att vi ställer relevanta frågor och ger bra svarsalternativ.

För att göra vår enkät använde vi oss av tjänsten Webbankäter.com som är ett verktyg för att skapa enkäter online. Med hjälp av webbankäter kunde vi genom ett smidigt gränssnitt enkelt välja vilka typer av frågor vi ville ställa och hur vi ville att frågorna skulle vara uppbyggda. Till exempel som “ja/nej” frågor, flersvarsfrågor, egen text o.s.v. En orsak till varför vi valde Webbankäter var för att det även ingår ett utvärderingsverktyg som gör det möjligt för oss att analysera svaren och få fram statistik från enkäten. Förutom detta kunde vi även välja att lägga till vissa begränsningar, som till exempel att en person bara kan svara en gång. Denna begränsning går till genom att en “cookie” lagras på deltagarens dator som har koll på om enkäten har besvarats av personen innan eller inte. Detta var en viktig funktion för oss då enkäten skulle spridas på internet och på så sätt kan vi minska risken att resultatet blir manipulerat.

4.2 Urval & spridning

Vi vill få reda på hur olika betalningsmedel står sig i Sverige idag och hur människor upplever risker kring dessa. Därför blir studien ganska allmän och riktar sig mot alla som någon gång har utfört betalningar på olika sätt. Genom att rikta studien till bred publik och inte mot en

specifik en grupp kan vi bland annat få fram svar från olika åldrar. På så sätt kan vi även använda svaren för att få fram olika typer av mönster, som till exempel för att se om ett visst betalningsmedel är vanligare bland en viss ålder. Studien är endast till för konsumenter, d.v.s. de som använder betalningsmedel i sitt vardagsliv för att handla med och inte för företag.

För att sprida vår enkät till så många som möjligt i varierande ålder har vi använt oss av internet. Där vi spridit den på sociala nätverk som till exempel Facebook och även på olika forum. Eftersom de flesta personer någon gång har utfört betalningar så är sannolikheten stor att många redan har en uppfattning och kan relatera till vårt ämne. Därför anser vi inte att spridningen behöver inrikta sig till ett specifik diskussionsforum. Vi kan därmed sprida enkäten till de flesta forum som tillåter det. Webbenkäter ger oss inte bara möjligheten till att skapa vår enkät, utan de tillåter oss även att publicera den på deras hemsida bland "offentliga enkäter" och med hjälp av dem kan vi nå ut till ännu fler.

Vi har även spridit den på Göteborgs Universitets lärplattform där vi skickat ut den till systemvetare från alla årskurser. Vi har även efter behov av fler svar skickat ut mail till vänner för att komplettera de befintliga svaren.

4.3 Metod för att analysera data

För att analysera datan från enkäten har vi att använt det utvärderingsverktyg som finns tillgängligt på webbenkäter. Genom att använda detta kunde vi direkt på hemsidan få fram statistik på hur respondenterna har svarat och även sortera svaren för att till exempel se hur en specifik åldersgrupp har svarat på en av våra frågor. På detta sätt kan vi se om det har uppkommit olika mönster, som till exempel skillnader och likheter mellan hur de olika åldersgrupperna har svarat.

Vi börjar enkäten med att se hur respondenterna upplever de risker som vi tagit fram, men vi ger även möjligheten för respondenten att lägga till egna risker kring de olika betalningsmedlen. De risker som vi tagit upp i teorin har vi valt att kategorisera (se Tabell 2) och på liknande sätt görs även en kategorisering av de risker som respondenterna har angivit i fritext. På så sätt kan vi jämföra kategoriseringen från teorin med den vi fått fram från enkätanalysen och därmed se vad för nya risker som tillkommit.

4.4 Validitet & Reliabilitet

Validitet

Validitet är ett begrepp som handlar om att man undersöker det man faktiskt avser att undersöka. I vårt fall handlar det om hur väl vår enkät svarar på vår frågeställning. Ett sätt att säkerställa validiteten är att man kollar på innehållsvaliditeten, vilket går till genom att man oftast kopplar den teoretiska ramen till undersökningen (Patel & Davidson, 2011). För att

säkerställa att vår enkät är av god innehållsvaliditet har vi valt att först studera litteratur och annan material från elektroniska källor kring ämnet. Detta har vi sedan använt för att kunna formulera frågor i vår enkät på ett sådant sätt att människor förstår vad vi syftar på.

Reliabilitet

Reliabilitet handlar om hur väl ett instrument (i vårt fall enkät) kan motstå olika slag av slumpinflytanden. Det svar vi får från en individ kan man kalla för ett "observerat värde", det observerade värdet innehåller både individens "sanna värde" och individens "felvärde". Där felvärdet kan bero på brister i instrumentet, till exempel att någon fråga misstolkas (Patel & Davidson, 2011).

Det kan vara svårt att se om en enkät är reliabel eller inte, utan det ser man egentligen inte förrän enkäten har blivit besvarad. Det är först då man kan se om det finns frågor som många har hoppat över, att fler alternativ kryssats i än vad man bett om eller missat att ta med vissa alternativ i enkäten. Patel och Davidson (2011) skriver att frågorna ska ställas på ett sådant sätt så att respondenterna uppfattar dem på samma sätt som vi gör. Det man också behöver göra är att man ger tydliga instruktioner genom hela enkäten om hur frågor skall besvaras (Patel & Davidson, 2011). Detta har vi gjort genom att vi har skrivit hjälptexter vid frågor som hjälper respondenterna att förstå till exempel vad ett visst begrepp betyder, eller att vi tydligt visar att man kan markera flera svar på en och samma fråga. I likhet med detta har vi utformat enkäten på så sätt att det inte går att markera flera alternativ vid de frågor som vi endast vill ha ett svar på. Ifall vi har missat att ge alternativ som respondenten anser borde ha varit med på en fråga, har vi gett dem möjligheten att skriva egna alternativ i fritext. Avsikten är att på sätt få ett mer reliabelt resultat. Eftersom vi sprider enkäten på internet finns det en risk med att någon förstör genom till exempel att svara på enkäten flera gånger, vilket på så sätt skulle manipulera resultatet. För att motverka detta har vi satt en begränsning så att man endast kan utföra enkäten en gång. Efter att man har svarat på enkäten så sparas en "cookie" på deltagarens dator som har koll på om enkäten har besvarats av personen innan eller inte.

5. Resultat

Resultatet av studien kommer att presenteras i form av diagram med tillhörande beskrivningar. Eftersom vissa av våra frågor har alternativet "ingen åsikt" kan antalet totala svar variera på frågorna. I några av våra diagram görs det olika typer av jämförelser, till exempel på hur olika åldersgrupper har svarat på en fråga. Från enkäten som vi spred på internet fick vi 156 svar, där 31 % av deltagarna var kvinnor och 69 % män och nedan i Tabell 3 visas åldersfördelningen hos de 156 som har svarat på enkäten.

- 15-25 år 93 svar
- 26-35 år 29 svar
- 36-45 år 14 svar
- 46-60 år 18 svar
- 61 år eller äldre 2 svar

Tabell 3. Åldersfördelning

5.1 Betalningsmedel som används och varför

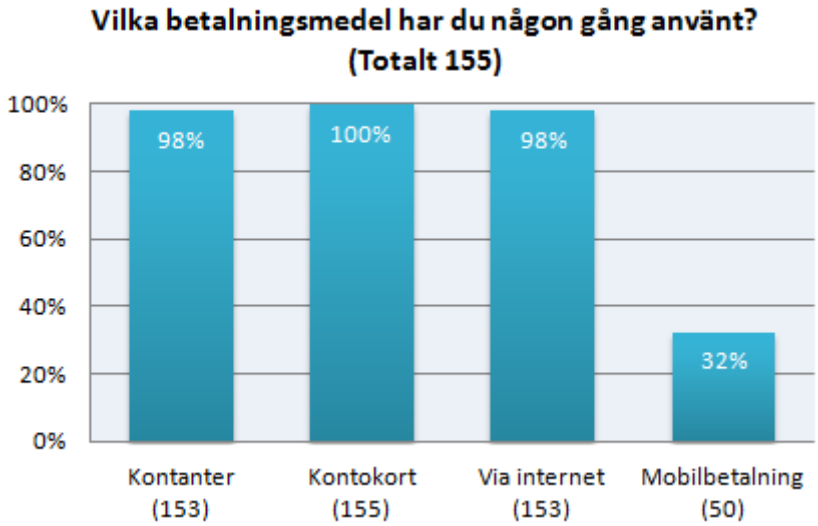

Diagram 1.

Diagram 1 visar vilka betalningsmedel som våra respondenter någon gång har använt. 98-100% av de tillfrågade har någon gång använt sig av kontanter, kontokort och internetbetalning. Medan endast 32 % någon gång har använt sin mobil för att betala.

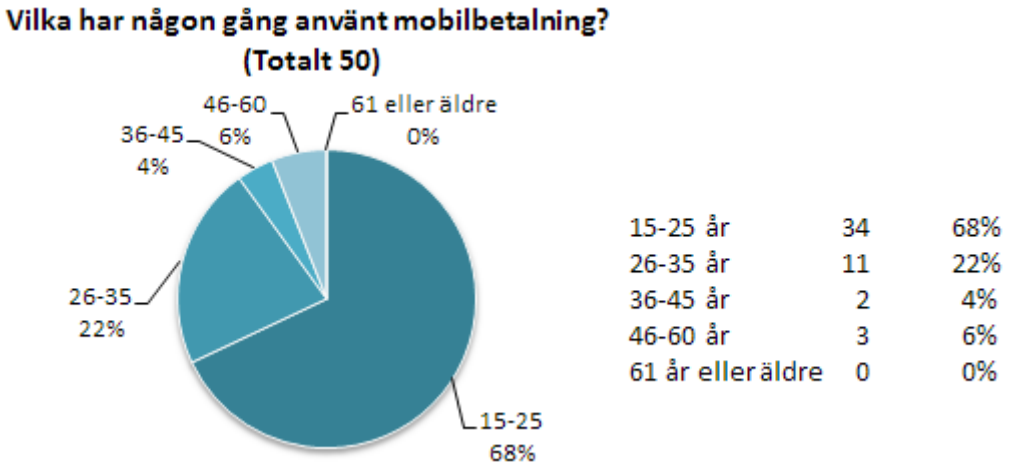

Diagram 2.

Eftersom det visade sig i Diagram 1 att det endast var 32 % som någon gång har använt sin mobil i betalningsammanhang valde vi att analysera hur åldersgruppen såg ut för de 32 procenten. I Diagram 2 kan vi se att majoriteten bland de som har använt mobilbetalning är i åldrarna 15-25, där 68 % är i denna åldersgrupp och 22 % är mellan 26-35. Medan de äldre svarar att de inte har använt sin mobil för att betala.

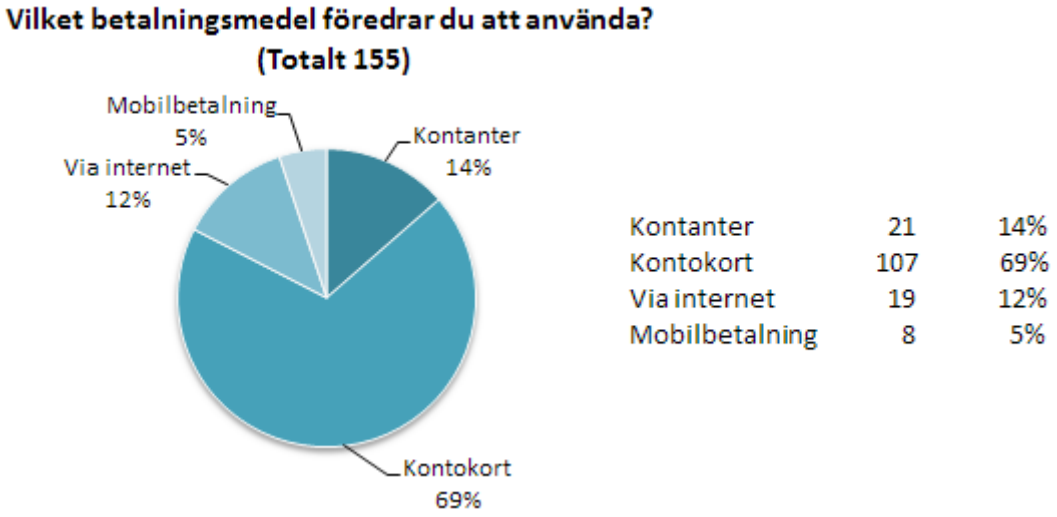

Diagram 3.

I relation till Diagram 1 där vi ställde frågan om vilka betalningsmedel de någon gång har använt, valde vi även att fråga vilket av dessa de främst föredrar att använda. Detta kan vi se i Diagram 3 som visar att mer än tre fjärdedelar (69 %) föredrog kontokort som betalningsmedel. De resterande betalningsmedlen var inte lika populära.

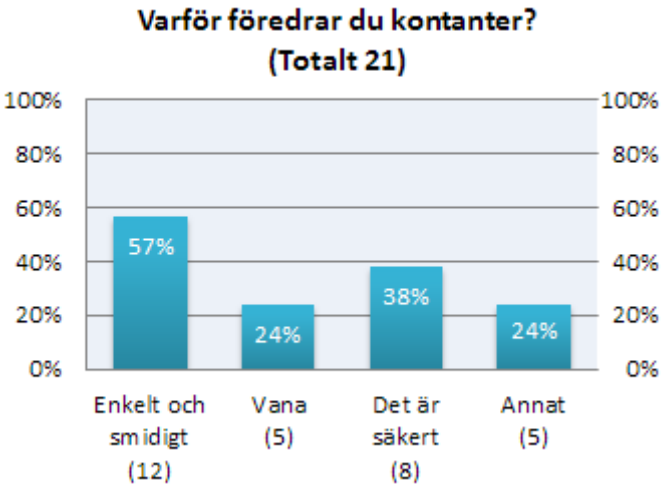

Diagram 4.

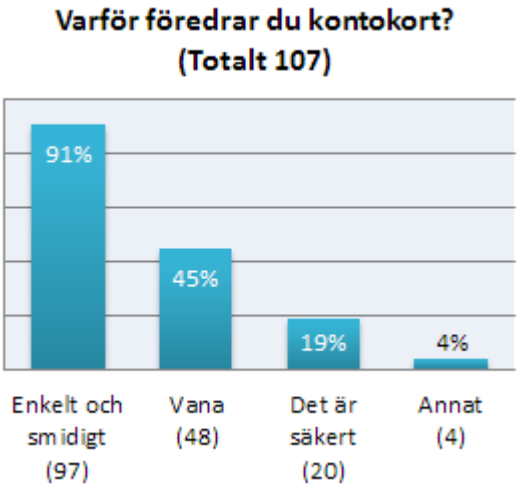

Diagram 5.

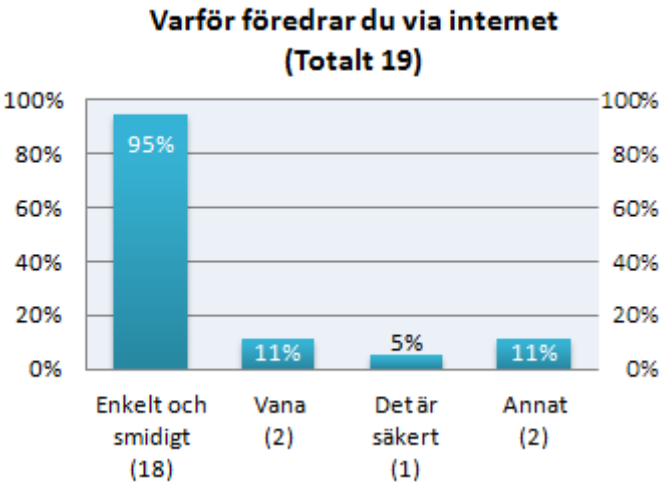

Diagram 6.

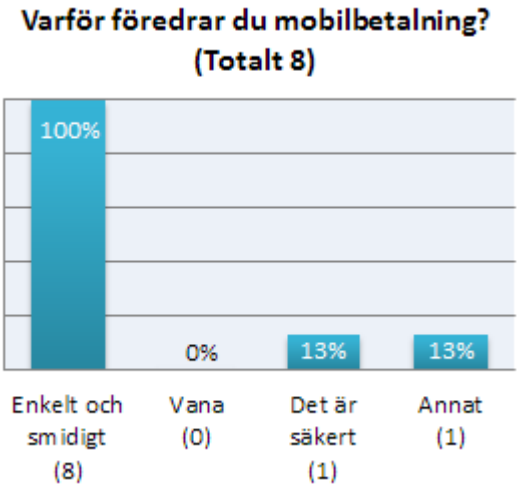

Diagram 7.

Dessa fyra diagram ovan (Diagram 4,5,6 och 7) visar för respektive betalningsmedel varför de föredrar just det betalningsmedlet. Det som nästan alla har gemensamt är att enkelheten och smidigheten hos ett betalningsmedel är en stor bidragande faktor. Förutom vid kontanter, där inte lika många svarar enkelt och smidigt (57 %) jämfört med de andra tre som ligger över 90 %. Det vi också kan se är att 45 % av de som använder kontokort gör det för att det har blivit en vana.

Varför föredrar du detta betalningsmedel? Öppna svar.

Kontanter
- *Integritetsskydd.* - *Varför byta ut ett fungerande system? Kort är för osäkert, lätt att få tag på andras konto information.* - *Integritet. Ingen ser vad jag handlar.* - *För att inte hamna i situationer där jag inte kan betala med kort.* - *Har bättre koll på pengarna på kontot.*
Kontokort
- *Har ett kort till allt. Slipper ha flera olika sedlar och mynt som tar plats.* - *Slipper hantera cash.* - *Slipper hålla ordning på kvitton.* - *Sällan kontanter på mig, oberoende var jag handlar finns det oftast möjlighet att betala med kontokort.*
Internetbetalning
- *Det går väldigt snabbt och man slipper resa på röven!* - *Behöver inte plocka fram något, har memorerat kontokortsnumret.*
Mobilbetalning
- *Alla borde våga gå över till sin mobil helt och hållet. Mha BankID och säkra bank-appar är det både smidigt och säkert att betala för sig.*

Tabell 4. Varför föredrar du detta betalningsmedel? Öppna svar

I Tabell 4 visas de öppna svaren från frågan om varför man föredrar ett betalningsmedel. Hos de som svarat att de föredrar kontanter säger vissa att det bland annat beror på att de vill skydda sin integritet. Samt att de vill undvika att hamna i situationer där de inte tar emot kortbetalning. Vid kontokort kan vi se att en del föredrar detta då de slipper att ha koll på kvitton, mynt och sedlar som tar plats. Vid internet och mobilbetalning kan vi även här se att enkelheten och smidigheten är en stor bidragande faktor för valet av betalningsmedel.

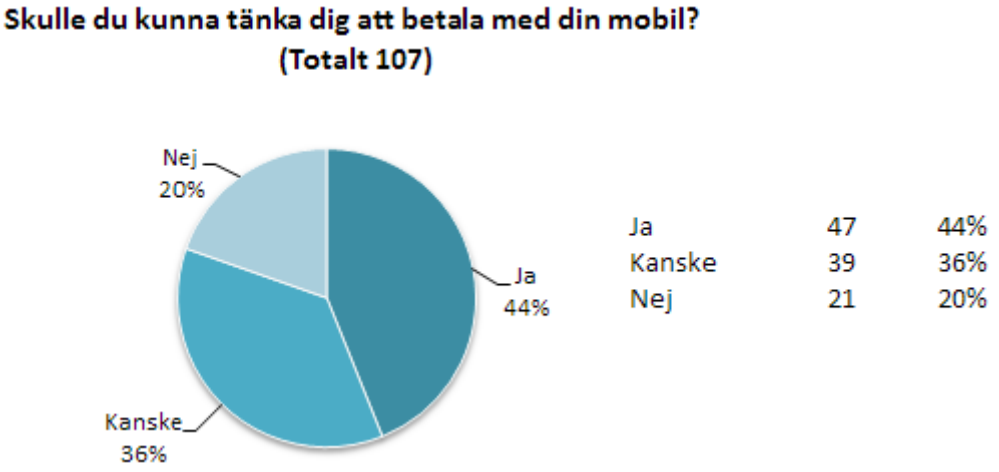

Diagram 8.

Med tanke på att mobilbetalning blir allt mer vanligt och att det dyker upp nya tjänster som gör det möjligt att använda sin mobil för att betala, valde vi att se hur stort intresset är för att använda sin mobil till detta ändamål. Det vi kan se är att 44 % kan tänka sig att betala med sin mobil, 36 % svarade kanske och 20 % ville inte alls betala med sin mobil (se Diagram 8).

5.2 Upplevda risker

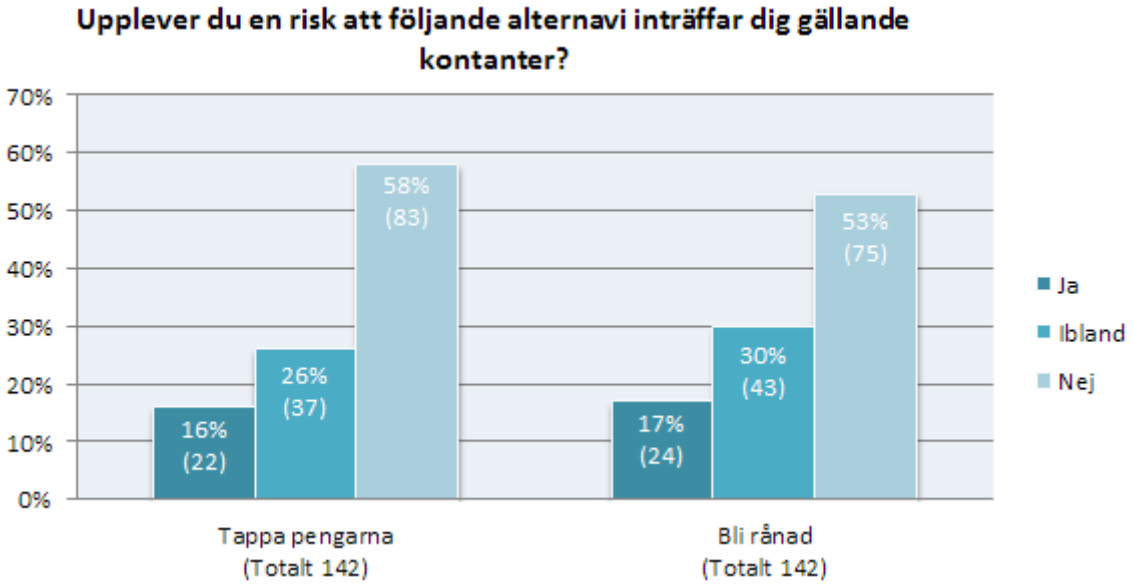

Diagram 9.

Här undersöker vi om respondenterna upplever att riskerna “tappa pengarna” och “bli rånad” skulle kunna inträffa dem gällande kontanter. Där endast 16 % upplever en risk för att tappa pengarna och 17 % upplever en risk för att bli rånad (se Diagram 9).

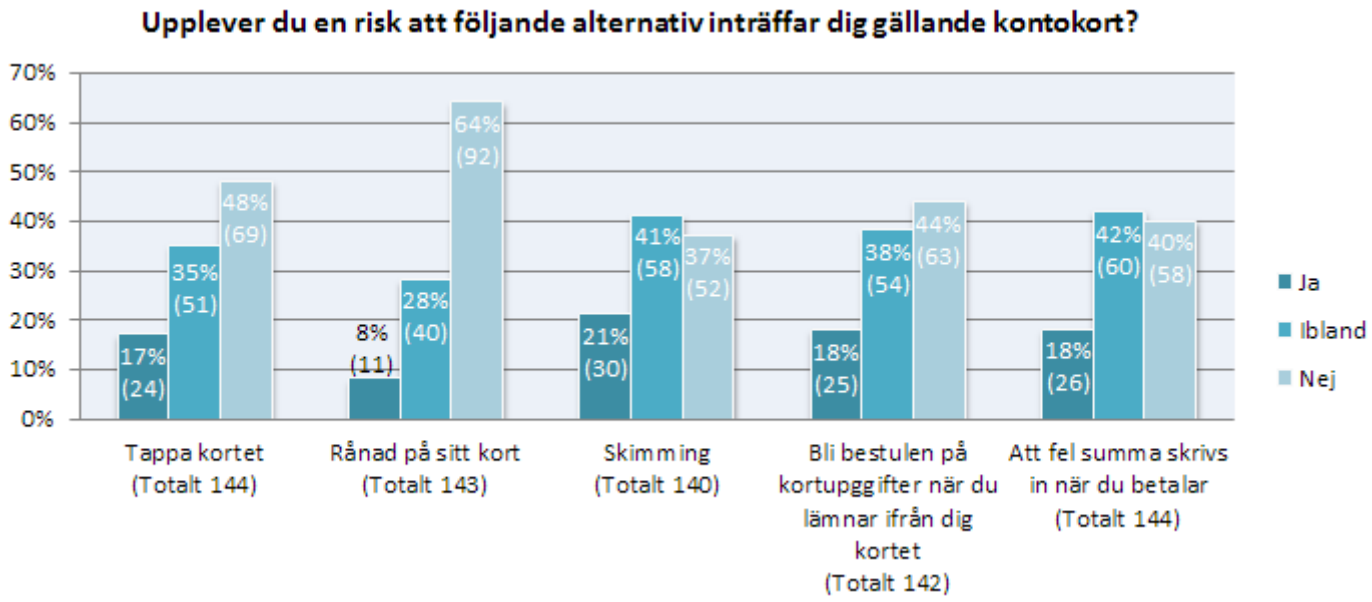

Diagram 10.

Diagram 10 visar hur respondenterna upplever olika risker gällande betalningsmedlet kontokort. Ungefär hälften av de tillfrågade upplever inte någon risk med att tappa sitt kontokort, men samtidigt svarar även 35 % att de ibland upplever denna risk. På frågan om man istället upplever en risk med att bli rånad på sitt kontokort, svarar hela 64 % nej. Gällande skimming är det lite mer osäkert, där närmare hälften (41 %) svarar att dem ibland upplever risken med att sitt kontokort kan bli skimmat. På de två sista riskerna gällande om man upplever en risk att ens kortuppgifter blir stulna när kortet lämnas ifrån, samt risken med att fel summa skrivs in, svarar majoriteten “ibland” och “nej”.

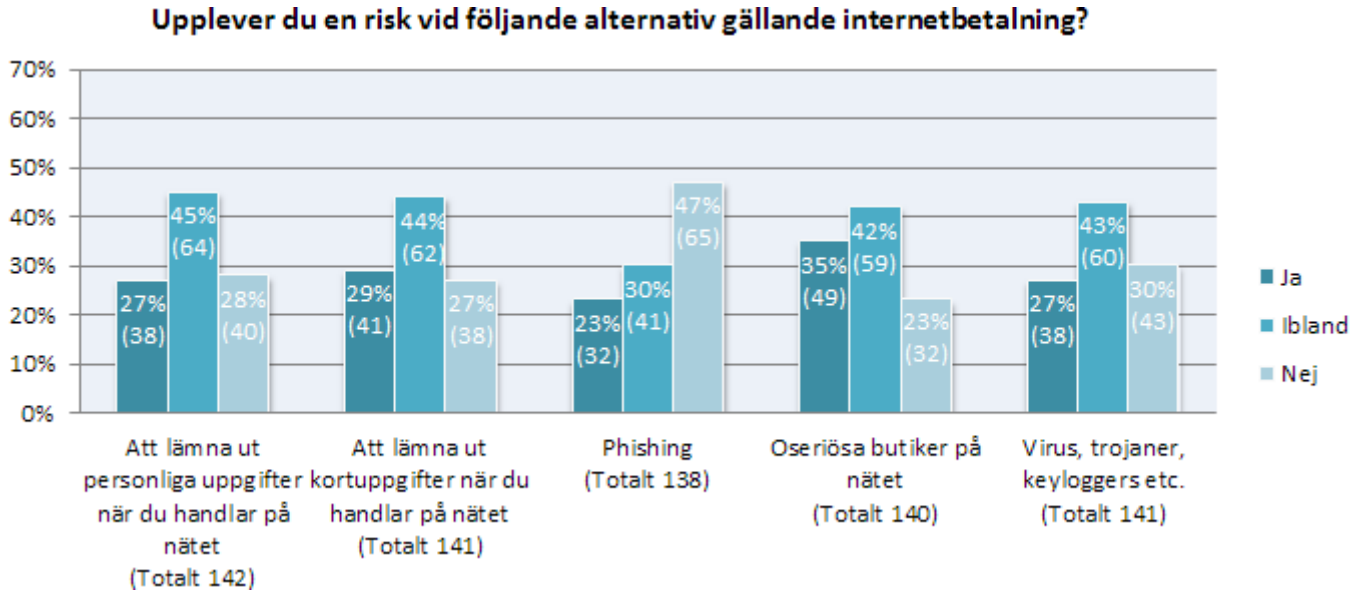

Diagram 11.

I Diagram 11 kan vi se hur respondenterna upplever olika risker vid internetbetalning. Det vi kan se är att 27 % upplever en risk när de skall lämna ut sina personliga uppgifter när de handlar på nätet och nästan hälften (45 %) säger att de ibland upplever det som en risk. På frågan om att lämna ut kortuppgifterna när de handlar ser siffrorna liknande ut som vid föregående risk. Gällande phishing svarar många att de inte upplever det som en risk, då 47 % svarar "nej", jämfört med endast 23 % som svarat "ja". På frågan om oseriösa butiker på nätet svarar endast 23 % "nej", medan majoriteten istället svarar "ja" och "ibland". Risken som handlar om virus som stjäl känslig information är det bara 27 % som upplever det som en risk, samtidigt är det många som är osäkra kring detta då 43 % svarar ibland.

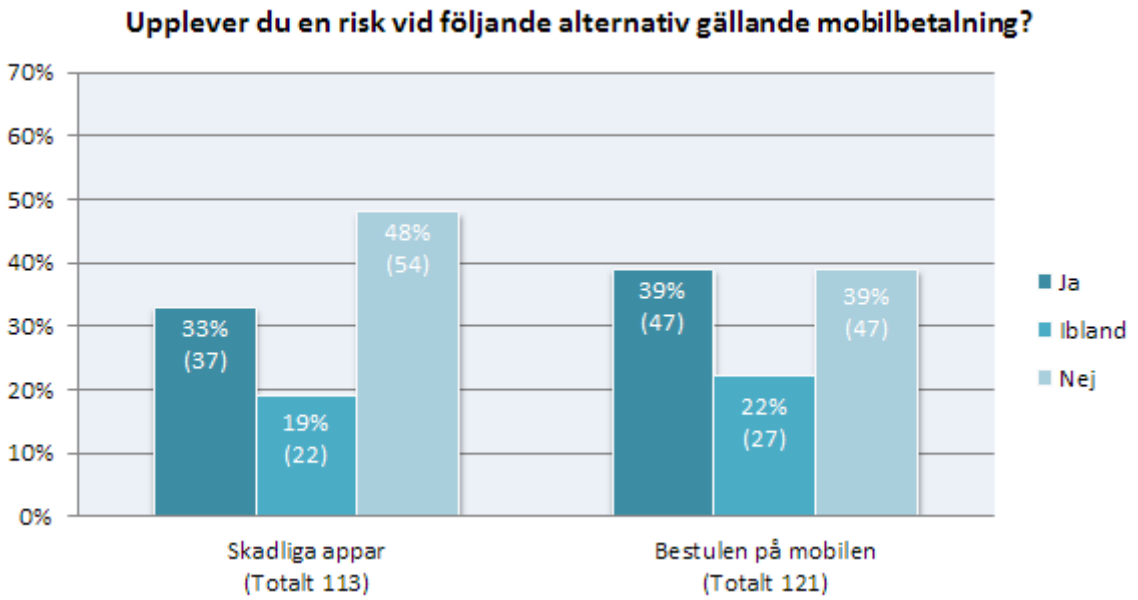

Diagram 12.

Diagram 12 visar om respondenterna upplever risker vid mobilbetalning. De risker som tas upp är "skadliga appar" som stjäl information, samt risken med att bli bestulen på mobilen som därmed kan ge tillgång till ens internetbank. Statistiken på dessa frågor är någorlunda jämt, 48 % anses inte uppleva någon risk för skadliga appar, medan 33 % gör det. På frågan gällande att mobilen blir bestulen svarar lika många "ja" som "nej" (39 %).

Upplevda risker vid betalningsmedel – En sammanfattning av de öppna svaren.

Kontanter
- *Överkonsumtion.* - *Att sedlarna går sönder.* - *Kontaminerade med bakterier(hygien).*
Kontokort
- *Att kortet blir obrukbart.* - *Tekniska problem.* - *Att kontokort inte accepteras som betalningsmedel.*
Internetbetalning
- *Bli av med kortuppgifter när de handlar eller gör bankärenden på internet.* - *Att av misstag skriva in fel uppgifter vid överförning av pengar.* - *Tekniska problem.*
Mobilbetalning
- *Bli av med känslig information (kortuppgifter och personuppgifter).* - *Tekniska problem som till exempel batteritid, mobiltäckning och liknande.*

Tabell 5. Upplevda risker vid betalningsmedel - Sammanfattning av de öppna svaren.

Tabell 5 visar en sammanfattning av dem öppna svaren från vilka risker respondenterna upplever kring de olika betalningsmedlen (se fullständiga tabeller i bilaga 2a). Det vi kan se är att många nämner risken för överkonsumtion när de har kontanter i plånboken, att man lättare spenderar sina pengar. En annan risk gällande kontanter är att sedlarna kan gå sönder och vara kontaminerade med bakterier. Gällande kontokort upplever många att det finns risk för tekniska problem eller att kortet på något sätt blir obrukbart. Samt att kontokort inte alltid accepteras som betalningsmedel. Vid internetbetalning svarar respondenterna bland annat att de upplever risker med att bli av med kortuppgifter när de handlar eller gör bankärenden på internet. De nämner även att de är rädda för att av misstag skriva in fel uppgifter och därmed överför pengar till fel konto, eller att tekniken inte fungerar. Slutligen för mobilbetalning skriver respondenterna att dem upplever en risk för att bli av med känsliga uppgifter, samt att man inte vill vara beroende av batteritid, mobiltäckning eller att det skulle kunna inträffa andra tekniska problem.

Upplevda risker vid internetbetalning (jämförelse)

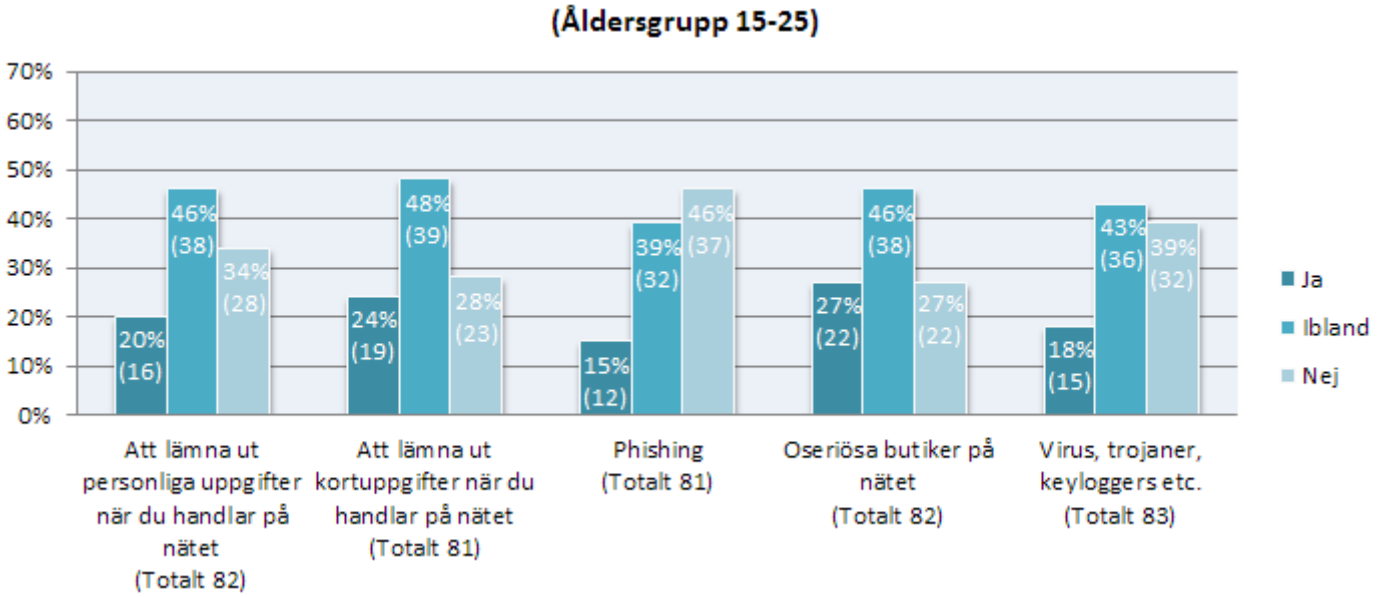

Diagram 13.

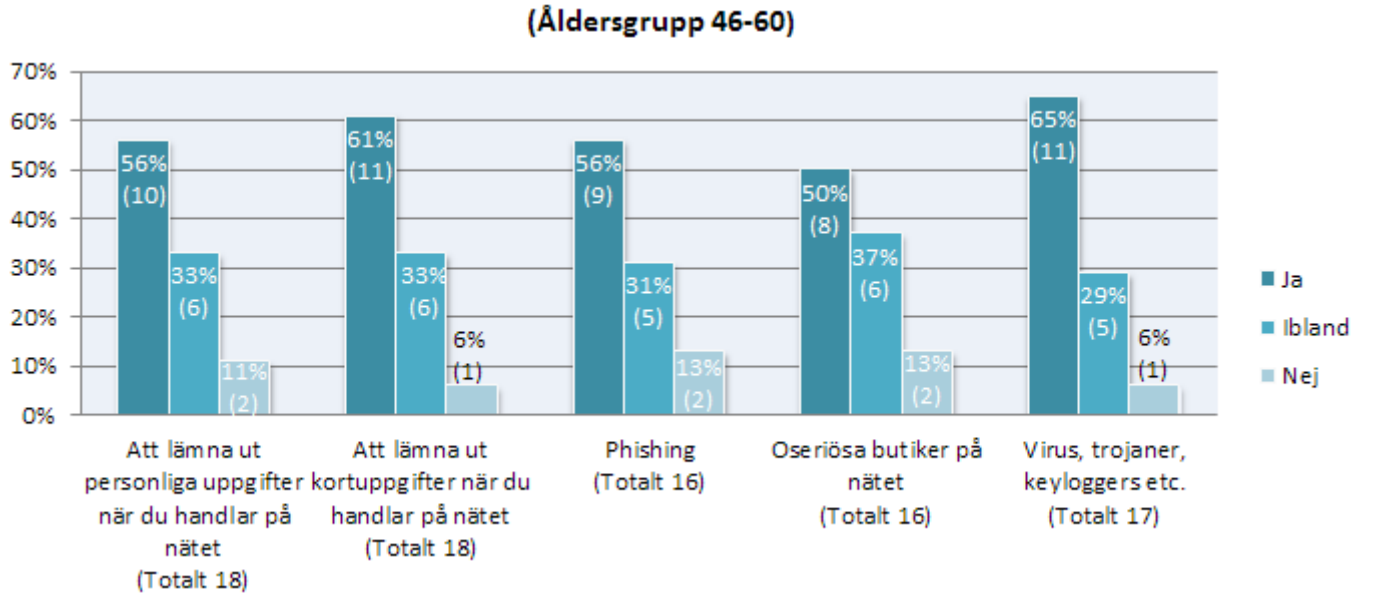

Diagram 14.

Här görs en jämförelse mellan Diagram 13 och 14, där vi ser hur två olika åldersgrupper har svarat på samma frågor gällande hur man upplever risker vid internetbetalning. Åldersgruppen som jämförs är 15-25 med den lite äldre 46-60. Vid åldersgruppen 15-25 som visas i Diagram 13 kan vi se att en relativt liten andel har svarat att dem upplever risker gällande internetbetalningar. Jämfört med den äldre åldersgruppen i Diagram 14, där statistiken ser helt annorlunda ut.

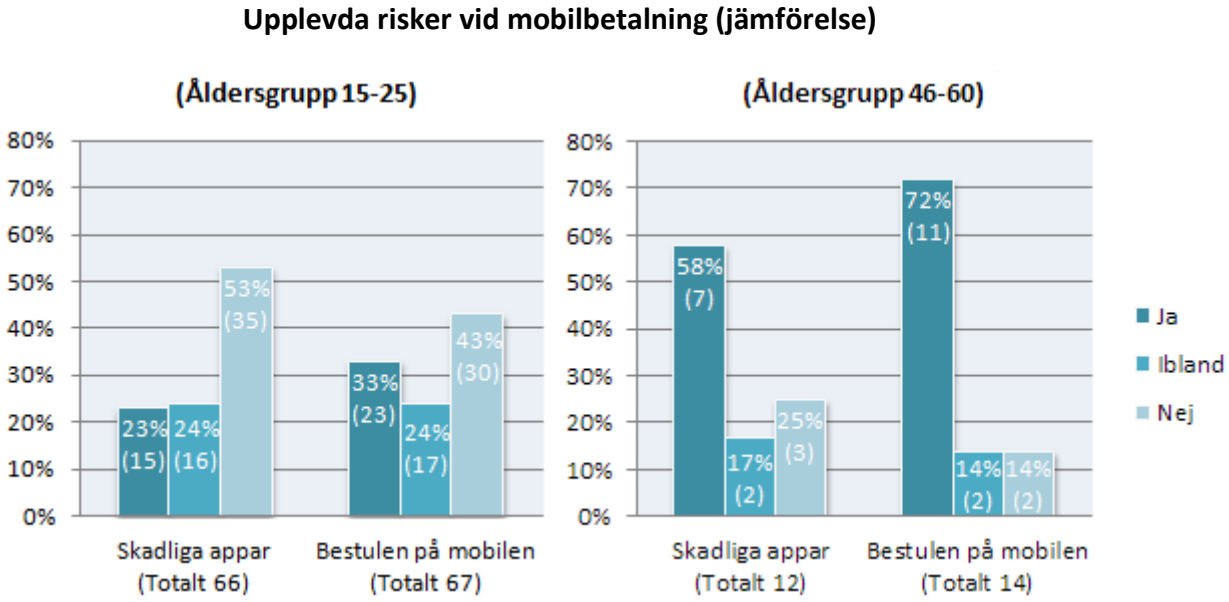

Diagram 15. *Diagram 16.*

I Diagram 15 och 16 kan vi se en jämförelse mellan samma åldersgrupper som i Diagram 13 och 14. Likt internetbetalning ser vi även här ett mönster där majoriteten av den yngre åldersgruppen har svarat att de inte upplever risker vid mobilbetalning. Medan majoriteten av den äldre åldersgruppen svarar att de istället upplever risker vid mobilbetalning.

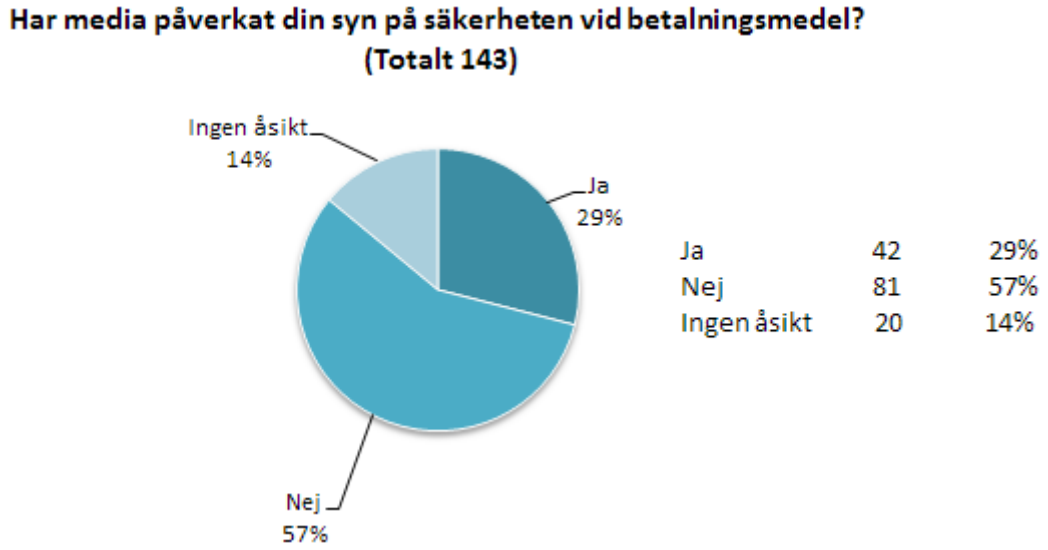

Diagram 17.

Eftersom det har skrivits en hel del om olika säkerhetsrisker gällande betalningsmedel i media på senare tid, ställde vi frågan “Har media påverkat din syn på säkerheten vid betalningsmedel?”. Det visar sig att 29 % av de tillfrågade anser att media har påverkat deras syn på säkerheten, medan 57 % svarar att de inte har påverkats (se Diagram 17).

Medias påverkan – En sammanfattning av de öppna svaren.
- *Allmänt försiktigare vid användandet av olika betalningsmedel.*
- *Kollar efter tecken på skimmingutrustning vid uttagningsautomater.*
- *Man är försiktigare när man kollar sina mail, för att undvika att det är bluffmail.*
- *Vissa anser att media överdriver, och tar därmed inte riskerna på så stort allvar.*

Tabell 6. Medias påverkan - Sammanfattning av de öppna svaren.

Tabell 6 innehåller en sammanfattning av respondenternas öppna svar på frågan om hur media har påverkat synen på säkerheten (se fullständig tabell i bilaga 2b). På grund av att risker har uppmärksammats i media, skriver dem att de i allmänhet blivit mer försiktigare vid användandet av olika betalningsmedel. Som till exempel att man alltid har uppsikt över sitt kontokort eller att de kollar efter tecken på skimmingutrustning vid bankomater. Vissa anser även att media endast överdriver och tar därmed inte riskerna på så stort allvar.

6. Diskussion & slutsats

För att besvara vår frågeställning valde vi att genomföra en enkätundersökning, vilket visade sig vara en bra metod för att få många svar. Tanken var att genom sprida enkäten på internet även kunna få svar från flera åldersgrupper. Detta gick inte riktigt som vi hade hoppats då majoriteten av respondenterna var mellan 15 och 25 år. Detta berodde mestadels på det sättet vi spred enkäten, genom bl.a. våra vänner på Facebook som för mestadels består av personer i 20-årsåldern och samt på forum som många ungdomar använder. För att vi skulle uppnå målet med att få svar från flera åldersgrupper kan man nu i efterhand se att det borde ha gjorts på ett annat sätt. Däremot anser vi att vårt resultat ändå är intressant eftersom vi kan se hur den yngre generationen tänker kring betalningsmedel och dess risker. Ett mönster som vi kan se är att de yngre överlag inte upplever risker i samma utsträckning som de äldre när det gäller de tekniska betalningsmedlen. En anledning till varför vi tror att det är så här kan vara för att den yngre generationen är mer van vid tekniken och känner sig mer trygg vid användandet och därmed inte upplever riskerna på samma sätt som de äldre. En annan observation som vi gjorde var att 68 % av de som någon gång hade använt mobilbetalning bestod av den yngre generationen. Detta kan bero på att yngre är mer intresserade av att testa nya tekniska betalningslösningar, vilket kan tyda på att vi förmodligen kommer se mer av dessa i framtiden då det verkar finns ett intresse för detta.

6.1 Resultatdiskussion

Det vi tydligt kunde se från vår enkätundersökning var att majoriteten (69 %) föredrar att använda sitt kontokort när de utför betalningar. På vår fråga om varför de föredrar kontokort, kunde vi se att det till största del berodde på att de ansåg att det var enkelt och smidigt att använda. Men det som också kom fram från fritextsvaren var att det också berodde på missnöjet hos andra betalningsmedel, som till exempel kontanter. Där de skriver att de slipper hantera sedlar och mynt som tar plats, till skillnad från kortbetalning där det räcker att endast ha ett plastkort till allt. Men de som föredrar kontanter skriver att man lättare har kontroll på hur mycket man spenderar och att man anser det vara integritetsskyddande eftersom det inte går att spåra ens inköp. Internet och mobilbetalning fick bara 12 respektive 5 procent av svaren. Att endast 12 % föredrar internetbetalning var överraskande för oss, då vi hade förväntat oss ett högre antal. Vi misstänker att detta kanske skulle kunna bero på att många antog att betalningar som sker med kontokortet på internet gick under kortbetalning istället för internetbetalning. Vilket i så fall var en miss av oss, då vi möjligen borde ha förklarat detta på ett tydligare sätt. Samtidigt tror vi inte att resultatet har påverkats i sådan utsträckning att det skulle vara missvisande. Anledningen till varför endast 5 % har svarat mobilbetalning tror vi kan bero på att det inte har etablerats i Sverige än. Däremot tror vi att vi kommer se en ökning i framtiden, då det nu satsas mycket inom detta område. Detta kan vi även se från vår enkätundersökning där 44 % svarar att de kan tänka sig att betala med sin mobil. Om vi jämför vårt resultat med studien Telia gjorde 2011 där

det visade sig att 30 % kunde tänka sig detta. Utifrån detta kan vi se att allt fler blir intresserade av mobilbetalning, vilket vi tror kan bero på att allt fler idag har smartphones och att de används till en mängd olika aktiviteter utöver att endast ringa och sms:a med.

En stor del av vår studie handlar även om hur människor upplever risker kring de olika betalningsmedlen. I resultatet från enkätundersökningen kan vi se att de två riskerna som vi har tagit upp kring kontanter inte upplevs hos så många av respondenterna. Endast 16 % upplever en risk med att tappa pengarna, samt 17 % svarar att de upplever en risk att bli rånad på kontanter. Samtidigt kan vi se att en större del svarar att de ibland upplever risker kring dessa. Anledning till varför vi tror att fler har svarat "ibland" istället för "ja" kan vara för att det beror på situationen. Till exempel att det kan upplevas som en större risk vid innehavandet av en större summa kontanter jämfört med enbart en liten summa. Från fritextsvaren gällande kontanter (se Tabell 5) kunde vi se att flera av dem som hade svarat upplever en risk för överkonsumtion, d.v.s. att de lättare spenderar sina pengar. Andra risker som kom fram var att de uttrycker en oro för att sedlarna skall gå sönder, eller att de är kontaminerade med bakterier. Eftersom kontanter är ett fysiskt betalningsmedel är detta svårt att undvika, då sedlar och mynt cirkulerar bland många människor. Det innebär att de slits och lätt blir smutsiga.

I vår enkät ställde vi frågor om respondenterna upplever risker gällande kontokort. Det vi kan se från de svar vi fått gällande de risker som vi tagit fram, så är det bara en liten andel som faktiskt upplever dessa som risker (se Diagram 10). Den risk som upplevs av flest är skimming vilket vi tror kan bero på all den uppmärksamhet som det fått i media på senare tid. En annan risk som sticker ut är "rånad på sitt kort" som få upplever som en risk. Detta kan bero på att det känns tryggare och säkrare jämfört med kontanter, eftersom kortet är skyddat av en PIN-kod och går enkelt att spärra. I fritextsvaren skriver flera av respondenterna att de upplever riskerna: att kortet blir obrukbart, tekniska problem och att kort inte accepteras som betalningsmedel. Ett samband som vi kan se hos dessa risker är att man känner sig beroende av att tekniken fungerar och att kortet går att använda. I de fall där tekniken inte skulle fungera eller att kortet inte accepteras blir man utan betalningsmöjlighet om det inte går att betala på andra sätt.

Gällande internetbetalning är det många som svarar att dem ibland upplever risker med att lämna ut känslig information som personuppgifter och kortuppgifter på internet (se Diagram 11). En av anledningarna till varför det ser ut så här tror vi beror på att vissa hemsidor är mer välkända och man har därmed större förtroende hos dessa. Däremot om det handlar om en okänd hemsida tror vi att det kan finnas en viss osäkerhet om hemsidan är pålitlig eller inte. Detta kan vi också se från de svar som vi fick gällande oseriösa butiker på nätet, där många skriver att de känner en viss oro kring detta. Eftersom en hemsida kan se pålitlig ut, kan det vara svårt att veta om butiken är seriös eller inte. Om vi delar upp resultatet i åldersgrupper, ser resultatet väldigt olikt ut. Det finns en stor skillnad mellan hur yngre och äldre upplever

risker gällande internetbetalning (se Diagram 13 och 14). Majoriteten av de äldre upplever risker vid internetbetalning, till skillnad från de yngre som inte gör det. Detta kan bero på att den yngre generationen är mer van vid tekniken och känner sig mer trygg vid användandet och därmed inte upplever riskerna på samma sätt som de äldre. I fritextsvaren finner vi risker som handlar om rädslan att av misstag skriva in fel uppgifter som OCR-nummer och liknande vid överföring av pengar (se Tabell 5). Detta kan bero på att OCR-nummer består av en lång rad med siffror och kan därför vara svåra att skriva in.

På frågorna som handlar om risker kring mobilbetalning tar vi upp skadliga appar som stjäl information och risken med att bli bestulen på mobilen som därmed kan ge tillgång till ens internetbank. På frågan om skadliga appar visar det sig att nästan hälften inte upplever detta som en risk. Vi tror att detta kan bero på att det inte är en risk som har uppmärksammats, samtidigt som man har ett stort förtroende för tjänsterna där apparna laddas ner ifrån och därför tror man inte att apparna därifrån är skadliga. Gällande risken om att bli bestulen på mobilen svarar lika många "ja" som "nej" (39 %) om att de upplever detta som en risk (se Diagram 12). Vid jämförelsen av olika åldersgrupper kan vi även här se en stor skillnad på svaren mellan de yngre och äldre. Majoriteten av de äldre upplever risker vid mobilbetalning, medan majoriteten av de yngre inte gör det (se Diagram 15 och 16). Detta tror vi kan bero på samma anledningar som vi tidigare nämnde vid jämförandet av åldersgrupperna hos internetbetalning. Att det har med att den yngre generationen är mer bekväm och van vid tekniken och därmed inte upplever riskerna i samma utsträckning som de äldre. Riskerna som vi fått fram från fritextsvaren gällande mobilbetalning är att man upplever en risk med att bli av med känslig information. Detta kan bero på att man inte litar på tekniken eftersom mobiler kanske inte uppfattas vara lika säkra som datorer. En annan risk som kom fram handlade om tekniska problem som till exempel batteritid, mobiltäckning och liknande. När det handlar om betalningsmedel, så vill man kanske helst inte vara beroende av saker som batteritider och mobiltäckning.

De risker som tillkommit från enkätundersökningen har vi valt att sammanställa i en kategoriseringstabell nedan (se Tabell 7). Detta är en utökning av Tabell 2 som vi tidigare presenterat i teorin och är det resultat av risker som kommit fram från studien. Det har tillkommit en ny kategori som vi kallar för "tekniska problem" denna innefattar risker som har att göra med tekniska aspekter. Det har även tillkommit nya risker i de befintliga kategorierna. Riskerna som har tillkommit består av mer vardagliga risker som till exempel att sedlarna går sönder eller att man av misstag skriver in fel uppgifter vid överföring av pengar. Tabellen innehåller en slutlig kategorisering av alla de risker som vi fått fram genom studiens gång.

Fysisk hantering
- *Bestulen på kontanter, kontokortet eller mobilen.*
- *Tappa kontanter, kontokortet eller mobilen.*
- *Skimming.*
- ** Att sedlarna går sönder.*
- ** Att kontokortet blir obrukbart.*
- ** Att sedlar och mynt är kontaminerade med bakterier.*
- ** Att kontokort inte accepteras som betalningsmedel.*
- ** Överkonsumtion vid innehav av kontanter.*
Informationshantering
- *Lämna ut personliga uppgifter (internet och mobilbetalning).*
- *Lämna ut kortuppgifter.*
- *Phishing (nätfiske).*
- *Fel summa skrivs in (i butik).*
- ** Att av misstag skriva in fel uppgifter vid överföring av pengar.*
Skadlig programvara
- *Virus, trojaner, keyloggers etc.*
- *Skadliga appar.*
Oseriösa aktörer
- *Oseriösa butiker på nätet.*
- *Bestulen på kortuppgifter när du lämnar ifrån dig kortet.*
*** Tekniska problem**
- ** Magnetremsan eller chippet slutar fungera.*
- ** Att tekniken inte fungerar vid betalning på internet.*
- ** Tekniska problem vid mobilbetalning som till exempel batteritid, mobiltäckning och liknande.*

* Nya risker från de öppna svaren

Tabell 7. Slutlig kategorisering av risker

På frågan om media har påverkat respondenternas syn på säkerhet svarar 57 % att de inte har påverkats (se Diagram 17). De som svarat att de har påverkats skriver att de har blivit mer försiktigare vid användningen av olika betalningsmedel, eller att de kollar efter tecken på skimmingutrustning vid uttagningsautomater och så vidare. Några av de som svarat “nej” anser att media överdriver och tar därmed inte riskerna på stort allvar. Vi håller också med om att media ibland överdriver, men och andra sidan bidrar media med att upplysa människor om de risker som kan finnas.

6.2 Slutsats

Från studien kan vi se att nästan alla någon gång har använt de betalningsmedlen som vi tar upp, förutom mobilbetalning. Av dessa så föredrar majoriteten i alla åldersgrupper kontokort, bland annat för att många tycker att det är smidigt och enkelt att använda eftersom det räcker att ha ett kort till allt och att man slipper hålla reda på sedlar och mynt. Anledningen till varför det är så få som testat mobilbetalning tror vi kan bero på att det fortfarande är väldigt nytt och inte så utbrett i Sverige i dagsläget. Däremot så kan vi se att 44 % av respondenterna kan tänka sig att använd sin mobil som ett betalningsmedel i framtiden. Detta tyder på att det förmodligen kommer bli allt mer vanligt i framtiden med den typen av betalning.

De risker som har tagits fram i teorin och de som kommit fram från vår enkätstudie har vi valt att kategorisera, för att på så sätt lättare få en överblick på vad för typ av risker som upplevs. Kategorierna har vi sedan sammanställt i Tabell 7 som är en utökning av Tabell 2. Tabell 7 innehåller en slutlig kategorisering av de risker som kommit fram genom studiens gång. Dessa är uppdelade i: fysisk hantering, informationshantering, skadlig programvara, oseriösa aktörer och tekniska problem. Tekniska problem är en ny kategori som har tillkommit från enkätundersökning, samt att det tillkommit fler risker i de befintliga kategorierna. Riskerna som har tillkommit består av mer vardagliga risker som till exempel att sedlarna går sönder eller att man av misstag skriver in fel uppgifter vid överföring av pengar.

Det vi kan se är att det finns många olika risker som upplevs vid de olika betalningsmedlen. Där det ibland är situationen som spelar roll, eller hur van man är vid användning av tekniken. Risker är något som är subjektivt och beroende på vem man frågar kan svaren variera. Däremot är det många av riskerna som liknar varandra och är av samma karaktär, vilket vi också kan se i vår slutliga kategoriserings tabell.

6.3 Vidare forskning

Eftersom vår studie är utformad med hjälp av en kvantitativ undersökningsmetod är det svårt att komma in på djupet och få en riklig beskrivning om varför de känner som de gör och hur de faktiskt tänker kring detta. Därför skulle det vara intressant att göra en kvalitativ studie där det går att få mer substans i svaren för att lättare förstå sig på hur människor resonerar kring risker och betalningsmedel. En annan intressant del att forska vidare på skulle kunna vara att fokusera på en äldre åldersgrupp, eftersom vår studie mestadels fick svar från yngre personer. Detta kan man sedan jämföra för att se vilka skillnader och likheter som kan finnas mellan dem.

Referenser

Böcker & Tidskrifter

Cho, C., Kang, J., & Cheon, H J. (2006). *Online Shopping Hesitation.* CyberPsychology & Behavior. vol. 9:3, p. 261-274.

Delac, G., Silic, N., & Krolo, J. (2011). *Emerging Security Threats for Mobile Platforms.* MIPRO, 2011 Proceedings of the 34th International Convention, p. 1468-1473.

Heron, S. (2007). *The rise and rise of the keyloggers.* Network Security. vol. 2007:6, p. 4–6.

Mallat, N. (2006). *Exploring Consumer Adoption of Mobile Payments - A Qualitative Study.* Proceedings > Proceedings of Helsinki Mobility Roundtable. Sprouts: Working Papers on Information Systems, vol. 6:44.

Mishra, B. & Ansari, G. (2012). *Differential Epidemic Model of Virus and Worms in Computer Network*. International Journal of Network Security. vol.14:3, p. 149-155.

Ondrus J. & Pigneur Y. (2009). *Near field communication: an assessment for future payment systems.* Information Systems and E-Business Management (ISEB), vol.7:3, p 347-361.

Patel, R. & Davidson, B. (2011). *Forskningsmetodikens grunder: att planera, genomföra och rapportera en undersökning.* vol. 4., [uppdaterade] uppl. Lund: Studentlitteratur

Sharma, L., & Patidar, R. (2011). *Credit Card Fraud Detection Using Neural Network.* International Journal of Soft Computing and Engineering. vol. 1:NCAI2011.

Yu, Weider D., Nargundkar, S., & Tiruthani, N. (2008). *Phishing Vulnerability Analysis of Web Based Systems.*

Elektroniska källor

Apple. (2011). *Apple's app store downloads top 10 billion.* http://www.apple.com/se/pr/library/2011/01/22Apples-App-Store-Downloads-Top-10-Billion.html (Hämtad 2013-04-24)

Apple. (2013). *App store tops 40 billion downloads with almost half in 2012.* http://www.apple.com/pr/library/2013/01/07App-Store-Tops-40-Billion-Downloads-with-Almost-Half-in-2012.html (Hämtad 2013-04-24)

Dediu, H. (2013). *A more complete picture of the iTunes economy.* 9 januari. http://www.asymco.com/2013/01/09/a-more-complete-picture-of-the-itunes-economy/ (Hämtad 2013-04-24)

Eriksson, N. (2012). *Polisen varnar: Betala kontant.* Aftonbladet. 6 oktober. http://www.aftonbladet.se/nyheter/article15563246.ab (Hämtad 2013-04-05)

Findahl, O. (2012). *Svenskarna och internet.* https://www.iis.se/docs/SOI2012.pdf (Hämtad 2013-03-18)

GP. (2012). *Många kan ha drabbats av skimmare*. 16 november. http://www.gp.se/nyheter/sverige/1.1132587-manga-kan-ha-drabbats-av-skimmare (Hämtad 2013-04-9)

Ivarsson, A. (2010). *Från Compisdator till cashkort - 7 teknikfloppar att glömma.* IDG. 5 april. http://www.idg.se/2.1085/1.307900/fran-compisdator-till-cashkort---7-teknikfloppar-att-glomma?showGallery=true&img=1 (Hämtad 2013-04-29)

Kreditkortinformation. (utan årtal). *Chip och magnetremsa.* http://www.kreditkortinformation.se/chip-och-magnetremsa (Hämtad 2013-04-24)

Lindström, K. (2011). *Telejättarna går ihop om mobilbetalningar.* IDG. 18 november. http://www.idg.se/2.1085/1.417150/telejattarna-gar-ihop-om-mobilbetalningar (Hämtad 2013-03-14)

Lygre, Erlend Tangeraas. (2013). *Sena (52) betalte 85.507 kroner for en kebab i Oslo.* Tv2.no 21 mars. http://www.tv2.no/nyheter/innenriks/sena-52-betalte-85507-kroner-for-en-kebab-i-oslo-4011247.html (Hämtad 2013-04-09)

Mastercard. (utan årtal). *Din plånbok - nu digital.* https://paypass.com/online/Wallet/Home (Hämtad 2013-03-12)

Metro. (2013). *Expert: Mobil betalning en säkerhetsrisk.* http://www.metro.se/nyheter/expert-mobil-betalning-en-sakerhetsrisk/EVHmat!MBCB6cVACjI/ (Hämtad 2013-04-12)

PayPal. (utan årtal). *Såhär här betalar du på nätet.* https://www.paypal.com/se/webapps/mpp/buying-online (Hämtad 2013-04-25)

Rådmark, H. (2009). *Rätt väg till lyckad e-handel: Säkerhet och risker.* https://www.iis.se/lar-dig-mer/guider/ratt-vag-till-lyckad-e-handel/sakerhet-och-risker/ (Hämtad 2013-04-10)

Svenska BankFöreningen. (2010). *Kontanter är bra för brottslingar.* 18 oktober. http://www.swedishbankers.se/web/bf.nsf/$all/4B69277C1FCA7132C12577BD004583A0 (Hämtad 2013-04-09)

Svensk Handel. (2011). *Så handlar vi på nätet 2011 - Företag och konsumenter på en global e-handelsmarknad.* http://www.svenskhandel.se/Documents/Rapporter/2011/S%C3%A5%20handlar%20vi%20p%C3%A5%20n%C3%A4tet%202011.pdf (Hämtad 2013-04-24).

Swedbank. (utan årtal). *Mobilbetalning Bart.* (a). http://www.swedbank.se/privat/internet-och-telefontjanster/bart/ (Hämtad 2013-03-12)

Swedbank. (utan årtal). *Upptäck mobilbanken.* (b). http://www.swedbank.se/privat/internet-och-telefontjanster/mobilbanken/index.htm (Hämtad 2013-04-25)

Symantec. (2007). *Virus masker och trojaner.* http://www.symantec.com/region/se/corporate/sakerhetsskola_virus_maskar_trojaner.html (Hämtad 2013-04-11)

Telenor. (2012). *Betala med mobilen i sommar.* 14 maj. http://www.telenor.se/foretag/varfor-telenor/beep/losningar/betala-med-mobilen-i-sommar.html (Hämtad 2013-03-14)

Zirn, T. (2011). *Varannan betalar med mobilen inom två år*. IDG. 21 november. http://www.idg.se/2.1085/1.417351/varannan-betalar-med-mobilen-inom-tva-ar (Hämtad 2013-03-14)

Bilaga 1 - Enkät

Betalningsmedel och dess risker

Hej!

Vi är två studenter som läser sista terminen på det systemvetenskapliga programmet på Göteborgs Universitet, institutionen för tillämpad IT. Vi skriver just nu vår kandidatuppsats som handlar om betalningsmedel och vad för risker som människor upplever kring dessa.

Enkäten riktar sig till alla över 15 år och som någon gång har utfört betalningar på olika sätt. De betalningsmedel som tas upp är kontanter, kontokort, via internet och via din mobil. Frågorna kommer inrikta sig på hur du som person upplever risker kring dessa olika betalningsmedel, samt vilket du föredrar att använda.

Enkäten består av 17 frågor där 5 av dessa är valfria och tar ca 5 min att besvara. Din identitet och dina svar är helt anonyma. Kandidatuppsatsen kommer till sist att publiceras i GUPEA (Göteborgs Universitets Publikationer - Elektroniskt Arkiv) för vetenskapligt ändamål.

Om du har frågor kring enkäten går det bra att kontakta oss via mail, Christoffer: gusandchap@student.gu.se, Philip: gusrobph@student.gu.se.

Tack till alla som deltar!

Med vänliga hälsningar Christoffer och Philip.

Betalningsmedel och dess risker

1. **Ålder** *

- ○ 15-25
- ○ 26-35
- ○ 36-45
- ○ 46-60
- ○ 61 eller äldre

2. **Kön** *

- ○ Man
- ○ Kvinna

3. **Teknisk kunskapsnivå?** *

(Vad du själv anser)

	1	2	3	4	5	
Låg	○	○	○	○	○	Hög

Bilaga 1 - Enkät

4. **Vilka betalningsmedel har du någon gång använt? (Kan välja flera) ***

- [ ] Kontanter
- [ ] Kontokort
- [ ] Via internet
- [ ] Via mobilen (Ej sms)

5. **Vilket betalningsmedel föredrar du att använda? ***

(Allmänt vad du föredrar, dvs. oberoende på hur och var du handlar)

- ( ) Kontanter
- ( ) Kontokort
- ( ) Via internet
- ( ) Via mobilen

6. **Varför föredrar du detta betalningsmedel? (Kan välja flera) ***

- [ ] Enkelt och smidigt
- [ ] Vana
- [ ] Det är säkert
- [ ] Annat

7. **Skulle du kunna tänka dig att betala med din mobil? ***

(T.ex. i butiker)

- ( ) Ja
- ( ) Kanske
- ( ) Nej

Bilaga 1 - Enkät

8. **Upplever du en risk att följande alternativ inträffar dig gällande kontanter?** *

	Ja	Ibland	Nej	Ingen åsikt
Tappa pengarna	○	○	○	○
Bli rånad	○	○	○	○

9. **[Valfri] Har du någon egen risk som du upplever och vill lägga till gällande kontanter? Beskriv gärna.**

10. **Upplever du en risk att följande alternativ inträffar dig gällande kontokort?** *

	Ja	Ibland	Nej	Ingen åsikt
Tappa kortet	○	○	○	○
Rånad på sitt kort	○	○	○	○
Skimming (En form av kortbedrägeri där information som finns på ett kontokorts magnetremsa kopieras)	○	○	○	○
Bli bestulen på kortuppgifter när du lämnar ifrån dig kortet (t.ex. när du betalar)	○	○	○	○
Att fel summa skrivs in när du betalar	○	○	○	○

11. **[Valfri] Har du någon egen risk som du upplever och vill lägga till gällande kontokort? Beskriv gärna.**

12. **Upplever du en risk vid följande alternativ gällande internetbetalning?** *

	Ja	Ibland	Nej	Ingen åsikt
Att lämna ut personliga uppgifter när du handlar på nätet	○	○	○	○
Att lämna ut kortuppgifter när du handlar på nätet	○	○	○	○
Phishing (Försök till att stjäla känslig information t.ex. via bluffmail)	○	○	○	○
Oseriösa butiker på nätet (t.ex. där varor inte levereras)	○	○	○	○
Virus, trojaner, keyloggers etc (Som stjäl känslig information, t.ex. kortuppgifter)	○	○	○	○

13. **[Valfri] Har du någon egen risk som du upplever och vill lägga till gällande internetbetalning? Beskriv gärna**

Bilaga 1 - Enkät

14. **Upplever du en risk vid följande alternativ gällande mobilbetalning?** *

	Ja	Ibland	Nej	Ingen åsikt
Skadliga appar (Som stjäl t.ex. bankinformation)	○	○	○	○
Bestulen på mobilen (Som därmed kan ge tillgång till din internetbank)	○	○	○	○

15. **[Valfri] Har du någon egen risk som du upplever och vill lägga till gällande mobilbetalning? Beskriv gärna.**

16. **Har media påverkat din syn på säkerheten vid betalningsmedel?** *

- ○ Ja
- ○ Nej
- ○ Ingen åsikt

17. **[Valfri] På vilket sätt har din syn på säkerheten påverkats av media? Beskriv gärna.**

(T.ex att du avstår från att använda något betalningsmedel. Eller att du blivit försiktigare vid användandet)

Bilaga 2a – Öppna svar: risker

9. [Valfri] Har du någon egen risk som du upplever och vill lägga till gällande kontanter? Beskriv gärna. Antal svar: 27

- ”Jobbigt att bära omkring på kontanter. Väldigt osmidigt.”
-” Sämre kontroll på var pengarna tar vägen jämfört med kort. Större risk att man betalar fel

summa om man tex inte kontrollerar växeln”

-”Ibland när jag har druckit lite mycket läskeblask så kan jag bli väldigt glad och spendera dessa pengar jag inte har någon koll på alls! Detta anser jag vara en väldigt jobbig risk för individen. ”

- ”Meckigt att behöva ta ut etc. ”

- ”Bättre koll på ekonomin”

- ”Kontanter har en förmåga att ta slut mycket snabbare än pengar på ett konto. D.v.s. risk för överkonsumtion. ”

- ”Den absolut största risken med kontanter är att man tappar dem. Om man har lite större belopp i kontanter på sig kan man även känna sig aningen paranoid för att bli utsatt för stöld.”

- ”Hatar kontanter bara”

- ”Kan ej få växel tillbaka, eller ha växel tillbaka”

- ”Det finns alltid en risk att kontanter inte räcker till vid betalningstillfället - notan blev större än väntat, priset var högre än vad jag trodde, etc. Det finns en risk att kontanter inte accepteras (på bussar, i automater, etc) Att vara beroende av kontanter innebär ett beroende av fungerande, tillgängliga uttagsautomater som inte kostar extra att använda (stor risk t.ex. när man reser) ”

- ”Köper upp dem så fort jag får tag på dem. Borde gå att spärra sig från att konsumera vissa saker och tillfällen.”

- ”dom är äckliga”

- ”Bakterier”

- ”Sedlar kan gå sönder och kan vara kontaminerade av smittor.”

- ”Nej”

- ”Förfalskningar”

- ”Att det glöms bort. Cash money är inget jag har lite av direkt. ”

- ”Tunga fickor av alla mynt... ”

Bilaga 2a – Öppna svar: risker

- ”glömma pengar i fickan + tvättmaskinen = inte bra. att sedlar går sönder på mitten. ”

- ”slippa ta ut kontanter på bankomat. ”

- ”När man "bryter" exempelvis en 500-lapp så blir det lätt hänt att man använder upp pengarna lättare än om man skulle ha pengarna på kort är min åsikt. ”

- ”Att butiker mfl behöver hantera kontanter innebär ju en risk för dem, att bli rånade.”

- ”att inte ha kontanter när du står i kassan och skall betala”

- ”Om jag får för mycket kontanter och vill sätta in dom på kontot så tar bankerna snart inte i mot dom”

- ”nej”

- ”The main problem is that they are physical not digital so they can end up in the wash or if there is a fire they may be burnt. Yhey can be riped, can blow away in the wind and so on.

- stor plånbok med kontanter i bakfickan känns i vägen, därför föredrar jag kort”

11. [Valfri] Har du någon egen risk som du upplever och vill lägga till gällande kontokort? Beskriv gärna. Antal svar: 11

- ”När magnetremsan eller chippet slutar fungera. Kan vara jobbigt om det är kris och banken är stängd. ”

- ”Ungefär samma som som på fråga nio, dock blir det svårare att skriva in kod samt göra signatur. ”

- ”Att de slets lätt och ibland går sönder”

- ”De butiker som inte har betalningssystem med kort riskerar att förlora vinst. Kontokort är närmast en förutsättning i handeln vilket begränsar valfriheten.”

- ”Den största risken jag ser med kontokort är när man betalar via internet (inte internetbank) och måste lämna ifrån sig sina kortuppgifter. I övrigt så är man väldigt säker när man handlar med sitt kort.”

- ”Att det jävla kortet går sönder”

- ”Kort fungerar inte alltid pga av tekniska problem, utan kontanter står man utan betalningsmöjlighet Kostköp kostar ibland extra. Alla försäljare accepterar inte kort.”

- ”Känsliga banksystem, kortköp kan inte beviljas trots att pengar finns på kortet”

- ”Använder du backtrack, är uppkopplade på någon annans wifi och de andra personerna som är uppkopplade kan förlora sin information om du vet vad du gör, och du får tillgång till deras kort ID, den där 3siffriga koden, datumet då kortet går ut osv.. Tar inte mer än 5 minuter att få tag på.”

Bilaga 2a – Öppna svar: risker

- ”Risk att kortet inte funkar pga för lite pengar på kortet för att ta ut på bankomat (typ 99:-) samt att kortet antingen avmagnetiserats eller på annat sätt blivit obrukbart. Vissa ställen tar inte kortköp under ett visst belopp vilket är en risk till ogenomtänkta inköp eller inga inköp alls genomförs. En risk till är att alla ställen fortfarande inte tar kort utan endast kontant.. Detta är fyra stora svagheter enligt mig med kort.”

- ”nej”

13. [Valfri] Har du någon egen risk som du upplever och vill lägga till gällande internetbetalning? Beskriv gärna. Antal svar: 11

- ”Använder mig av nordeas "säkra kortbetalningar" när jag handlar på nätet. Det känns tryggt. ”

- ”risk for information security breaches IF my data is stored in a unsecure database

- ”Internetbetalning är ett såpass anonymt sätt att genomföra transaktioner. I förlängningen kan transaktioner komma att göras mellan konton istället för individer. ”

- ”De största riskerna jag ser med internetbetalning är stöld av kredituppgifter och personuppgifter. ”

- ”Att jag skickar till fel giro-nummer”

- ”Det finns alltid en risk att tekniken inte fungerar och det är ofta svårt och krångligt att kontakta kundsupport och bank för att lösa problemet och få bekräftelse på att köpet gått igenom, reservationen är accepterad, etc. ”

- ”Att internet ligger nere vid tex krig, eller naturkatastrof. ”

- ”nej! ”

- ”Jag kan noja mig över att jag skulle av misstag kunna skicka pengarna till fel konto eller fel summa vilket känns som en risk.. BTW är OCR-nummer PAIN IN THE ASS!! att fylla i (om det inte är via mail då man bara kan kopiera över skiten). Risken med OCR är att jag blir extremt irriterad över hur lång tid det ska behöva ta då jag måste dubbelkolla ett antal gånger då sifferkombinationen på OCR numret är längre än alla siffror i talet PI! (känns det som iaf..) Kan känna en viss risk när man köper utav privatperson på exempelvis Tradera då allt ansvar ligger hos en själv och säljaren att allt går till på rätt sätt. ”

- ”Tänker hela tiden på att minimera risken genom att "handla säkert" via internetbetalning”

- ”many games today require that you pay”

Bilaga 2a – Öppna svar: risker

15. [Valfri] Har du någon egen risk som du upplever och vill lägga till gällande mobilbetalning? Beskriv gärna. Antal svar: 6

- ”Har aldrig använt mobilbetalning så det är svårt att lämna en åsikt. Jag kan däremot tänka mig att jag skulle vara något orolig över att bli bestulen på mobilen om jag använde denna typa av betalning.”

- “Honey pot, where free and open wifi can be used to steal personel information”

- ”Att jag inte håller koll på min mobilräkning och får en jobbig räkning.”

- ”Nyare mobiler (smartphones) har ofta mycket begränsad batteritid och jag skulle inte vilja riskera att vara beroende av min mobil för betalningar. Mobilnäten har fortfarande relativt dålig täckning och problem med datatrafik, speciellt utanför större städer och på landsbygden. Jag skulle inte vilja vara beroende av mobiltäckning från min operatör för att kunna betala. Jag misstänker att det finns risk för tekniska problem av samma typ som kort och internet-betalningar.”

- ”nej!”

-” Betalar ej via mobil. Kan ibland boka saker, men inte mer än så.”

Bilaga 2b – Öppna svar: medias påverkan

17. [Valfri] På vilket sätt har din syn på säkerheten påverkats av media? Beskriv gärna. Antal svar: 24

- ”Kollar efter tecken på skimmingutrustning vid uttagningsautomater. Samt håller handen över när jag skriver in min pinkod. ”

- ”Att man är lite mer försiktigare när man fått luriga mail, som skulle kunna innebära att dom stjäl mina kortuppgifter (nätfiske). Att man är mer uppmärksam när man skall genomföra ett köp genom att kolla extra noga på vad som finns på sidan. ”

- ”Möjligen blir man lite mer betänksam men det har inte påverkat såpass att jag ändrat mina betalningsvanor. ”

- ”Tycker inte de har direkt påverkat mig så mycket. Det är väl mest egna påståenden och egna funderingar på hur säkerheten kan vara dålig.. ”

- ”man har hört om både skimming och phishing vilket många aldrig hört talas om tidigare. är man lite orolig av sig i allmänhet kan man ta dessa hot på stort allvar och ändra uppfattning till betalningsmedel. själv har jag noterat hoten men aldrig oroat mig i större grad då banker/försäkringsbolag kan ersätta mig + förkomsten av dessa brott känns låg”

- ”Blivit aningens försiktigare, men inte mycket”

- ”The news. Eg when Sony was hacked. Millions of accounts were stolen.”

- ”Media har påverkat mig på så sätt att jag inte längre brukar kontanter i samma utsträckning. ”

- ”Eftersom jag är utbildad inom IT-säkerhet så vet jag vilka risker det finns, troligt mycket bättre än vad media förstår sig på. Media kan inte påverka mig mer än att jag kan min egen säkerhet. ”

- ”Inte alls, media överdriver allt + att jag inte är pensionär så jag kan faktiskt hantera mig själv med mina betalmedel”

- ”Inget jag kommer på för tillfället. Men media har säkert gjort sitt i mitt undermedvetna.”

- ”Media har inte påverkat. ”

- ”Man har blivit mer försiktig i allmänhet när det gäller olika betalningsmedel.”

- ”Media rapporterar ofta om fall av intergritetskränkning i samband med elektronisk handel. Man rapporterar även mycket om riskerna med kontanthantering och risken för rån som uppstår hos t ex butiker som hanterar kontanter eller mot värdetransporter. Min bild av säkerheten för olika betalningssätt har främst formats av media, eftersom det trots allt är där man får majoriteten av sin information. Media har dock inte något egentligt mål att alltid rapportera objektivt utan styrs lätt av näringslivet och staten. ”

Bilaga 2b – Öppna svar: medias påverkan

- ”Det har blivit lite mer försöktigt när jag betalar. Information som handlar om skmming har jag fått från nyhet på nätet.”

- ”Använder e-kort för att minska risk. ”

- ”Vill veta vid inbetalning vad som dras direkt. Betalar via autogiro.”

- ”naturligtvis har man blivit försiktigare vid användandet”

- ”Att inte lämna kortet med ögonen.”

- ”Blir mer uppmärksam på tex skimning och bluffmail. Samt att vara restriktiv med att ge ut uppgifter.”

- Program som exempelvis PLUS”

- ”Ju mer man läser om oliks saker som kan hända desto mer orolig blir man”

- ”Upplysning ger kunskaper - tänker till lite extra - men avstår inte att använda kort- eller internetbetalningar”

- ”Man blir mer medveten om risken och blir försiktigare”