Högskolan i Halmstad
Sektionen för Informationsvetenskap, Data- och Elektroteknik
Informatik 61-90hp

PERSONLIG INTEGRITET OCH SÄKERHET I SOCIALA NÄTVERKSMILJÖER

Kandidatuppsats, 15 hp
Slutseminarium: 2010-05-27

Författare:
Madeleine Holgersson
Henrik Smederöd

Handledare**:** Carina Ihlström Eriksson

Förord

Det här är en kandidatuppsats i Informatik vid Högskolan i Halmstad. Uppsatsen är skriven våren 2010 vid utbildningarna Valfritt Informatikprogram och Multimediadesignprogrammet, tillhörande sektionen för Informatik, Data- och Elektroteknik.

Vi vill rikta speciellt tack till vår handledare Carina Ihlström Eriksson som har varit ett starkt stöd under hela processen och har uppmuntrat oss under arbetets gång. Vi vill också passa på att tacka de respondenter som deltagit i vår studie samt våra opponenter som har kommit med konstruktiv kritik under de seminarier som har hållits. Sist men inte minst vill vi tacka de studenter som har varit testpersoner för studien under dess utveckling.

Halmstad,

Madeleine Holgersson

Henrik Smederöd

Abstrakt

När sociala nätverk blir en del av människors vardag öppnar sig många möjligheter till interaktion med vänner, kollegor och bekanta på nätet. Medan sociala nätverk erbjuder en uppsättning av verktyg och forum för att dela med sig av vardagen kan de också utsätta användaren för risk gällande den personliga integriteten och säkerheten. Denna uppsats behandlar hur användare kan vidta försiktighetsåtgärder för att skydda sin personliga integritet och säkerhet på sociala nätverk. Med detta i åtanke genomfördes en kartläggning av tre sociala nätverk för att identifiera vilka risker som en användare kan utsättas för. Dessutom genomfördes en onlineundersökning där användare svarade på hur deras åsikter angående inställning, medvetenhet och beteende ter sig i givna situationer. Slutsatserna av studien resulterade i rekommendationer som kan ges till användare för att förbättra deras personliga integritet och ge en säkrare upplevelse av sociala nätverk, så som; Undersök vilka olika inställningar som finns tillgängliga för Ditt konto.

Nyckelord: sociala nätverk, integritet, säkerhet

Innehållsförteckning

1 Inledning

Inledningen syftar till att ge läsaren en introduktion till ämnet denna uppsats behandlar.

2000-talet har inneburit en stor förändring för hur människor interagerar med varandra genom att fler och fler har tillgång till Internet i sina hem samt att medierna för dessa interaktioner har blivit mer tillgängliga. Idag finns en mängd olika nätverk för att dela med sig av sitt jobb, sin fritid och intressen där bloggar, microbloggar, fotodagböcker etc. spelar en stor roll i människors vardag. Socialt nätverkande är ett begrepp som har inneburit en utveckling från att endast hålla kontakten med sina vänner via loggar och mail, till att se sina vänners dagliga förehavanden, att tagga vänner i foton, att använda applikationer inom nätverk där man får kontakt med människor som delar samma intresse etc. Enligt Gross och Acquisti (2005) kan sociala nätverkssajter delas in i flera kategorier, där bland annat affärsverksamhet, dating, gemensamma intressen, vänner och foton ingår. Enligt webbstatistik som utförs av Alexa [1] ligger sju respektive tolv sociala nätverk i topp 20 av besökta webbplatser under den senaste månaden i Sverige samt globalt, vilket tydliggör användandet av dessa tjänster.

Den stora ökningen i socialt nätverkande på Internet har lett till att diskussionen om integritet och säkerhet satt fart. *Integriteten* på sociala nätverk gäller huruvida användarna har kontroll över och inte blir kränkta av den personliga information som finns tillgänglig (Brodie, Karat, Karat & Feng, 2005; Danezis, 2009). Gemensamt för de olika kategorierna nämnda ovan är att de sociala nätverken kräver att du skapar ett användarkonto för att få tillgång till sajten. Vid skapandet av ett användarkonto måste en viss mängd personlig information uppges, hur mycket är varierande från nätverk till nätverk. Vissa delar av denna information kommer att vara tillgängliga för andra användare medan andra, mer känsliga delar av informationen lagras för unik identifiering samt betalningsfunktioner (Luo, Liu, Liu och Fan, 2009).

Säkerhet på sociala nätverk syftar till de verktyg och tekniker som används för att kontrollera vem som kan använda eller ändra informationen. Tillgängligheten till information på de sociala nätverken tilltalar tyvärr även kriminella organisationer som genom olika tillvägagångssätt letar upp värdefulla uppgifter (Joinson, 2008; Luo *et al.*, 2009; Saltzer & Schroeder, 1975). TechWorld [2] påstår att ”2009 var året då sociala nätverk på allvar började utnyttjas av kriminella på Internet” och att det grundar sig på människors villighet att lämna ut information om sig själva på ett helt annat sätt på Internet än vad de hade gjort i verkliga livet.

Schrammel, Köffel och Tscheligi (2009a) menar att även om användaren inte måste lämna ut flertalet uppgifter så väljer de att ändå göra det för att få full tillgång till de sociala funktioner som finns att tillgå. De funktioner som kräver att mer information lämnas har många gånger antingen en varningstext eller ett licensavtal kopplat till sig som skall ge användaren information om vad tjänsten innebär. Dock är dessa texter vanligen skrivna med ett byråkratiskt språk och i ett kompakt format som gör dem jobbiga att läsa och svåra att förstå. Åtskilliga användare är på

grund av detta inte fullt medvetna om de risker och konsekvenser som kan följa av deras handlande, eller vem som får tillgång till informationen de publicerar (Krishnamurthy & Willis, 2008). Relationen mellan privatliv och användande av sociala nätverk är väldigt tunn som Chen och Shi (2009) påpekar. Tilliten användare har till de sociala nätverken samt villigheten att lämna ut information för att få tillgång till alla funktioner gör användarna till en utsatt grupp som de kriminella inte är sena att utnyttja.

Det utbredda intresse som finns idag för sociala nätverk där användare bidrar till innehållet gör att den höga uppgiftsutlämningen är en risk både för den personliga integriteten och för säkerheten. Därför ställer vi oss frågan:

Hur kan användare vidta försiktighetsåtgärder på sociala nätverk för att skydda sin personliga integritet och säkerhet?

Syftena med denna uppsats blir således att:

- Kartlägga vilka funktioner och aktiviteter som kan innebära ett hot mot användarens integritet och säkerhet på sociala nätverk.
- Undersöka användarnas inställning till integritetsfrågor, medvetenhet om säkerhetsrisker samt påstådda beteende på sociala nätverk.
- Bidra till att öka medvetenheten hos användare på sociala nätverk genom rekommendationer.

2 Teori

I detta kapitel presenteras den teoretiska referensram som byggts upp av litteraturstudierna. Avsnittet definierar begreppen sociala nätverk, integritet och säkerhet, samt presenterar djupare kunskap inom delar av dessa områden, vilka är relevanta för uppsatsen.

2.1 Sociala nätverk

Sociala nätverk i det verkliga livet är en struktur mellan aktörer som indikerar hur de är kopplade till varandra genom olika sociala bekantskaper, oftast är dessa aktörer individer eller organisationer. Till de sociala nätverken kan bland annat posttrafik och telefonsamtal höra, men även sådant som kriminella aktiviteter räknas dit då kommunikationen kriminella emellan kan ses som ett nätverk (Jamali & Abolhassani, 2006).

Online sociala nätverk kan definieras som communities på Internet där individer interagerar och kommunicerar genom profiler som representerar dem själva och deras kontakter till andra (Acquisti & Gross, 2006). Datorstödda communities har funnits sedan 1960-talet men det är inte förrän Internet kom som de mötte intresse från den publika sektorn. Redan på 1990-talet fanns många communities för intresserade användare där vissa växte snabbare än andra. Den växande marknaden var något som även media och den akademiska världen lockades av och valde att integrera med, vilket har gett upphov till nätverk som Facebook [3] (Gross & Acquisti, 2005). När sociala nätverk omnämns hädanefter kommer det att syfta till de sociala nätverken online.

De sociala nätverkens användare har ökat enormt under de senaste åren (Danezis, 2009). Facebook [3] har från att i mitten av 2007 ha 30 miljoner användare (Joinson, 2008) gått till att 2010 ha fler än 400 miljoner användare [4]. Även andra sociala nätverk som MySpace redovisar över 100 miljoner användare 2008 (Joinson, 2008; Schrammel *et al.*, 2009a) och har i januari 2010 nästan 70 miljoner användare bara i USA [5]. Nätverkens ökning har gett användare större möjlighet att interagera internationellt.

Användare interagerar med varandra på de sociala nätverken genom att söka efter människor genom olika kriterier. Sökningen är genomförbar tack vare de profiler som varje användare skapar när de skapar ett användarkonto (Luo *et al.*, 2009), där de sociala nätverken uppmuntrar att profilerna innehåller information så som namn, födelsedag, intressen osv. Informationen som användarna ger och söker efter kan sedan leda till att grupper skapas där användarna har ett eget forum för diskussion, skapande av information om arrangemang och uppladdning av fotografier (Joinson, 2008).

Sociala nätverk kan också ge samma support som användarna får i det verkliga livet såsom att de får stöd både emotionellt och socialt från vänner i nätverket, att de kan knyta nya kontakter eller att de får tillgång till information som annars skulle ha varit utanför deras kännedom (Joinson, 2008). Det finns även andra anledningar till användandet av sociala nätverk. Lampe, Ellison och Steinfield (2006) menar att det finns två typer av användare; social searchers som använder

nätverken för att hålla kontakt och få information om människor de har en offline-kontakt med och social browsers som använder nätverken för att hitta nya kontakter som de skulle vilja ha en offline-kontakt med. Cutillo, Molva och Strufe (2009) säger att huvudorsaken till användande av sociala nätverk är att dela information med andra av någon anledning, vilken information som delas beror på vilket nätverk man går med i och kan delas in i två delar; att dela privat information eller att dela professionell information, där Facebook [3] kan kategoriseras som ett nätverk där man delar privat information och LinkedIn [6] är ett nätverk för affärsverksamheter och professionell information.

Användare som väljer att dela med sig av professionell information gör detta oftast för att etablera affärskontakter och väljer nätverk med yrkesmässig inriktning. De användare som väljer att dela med sig av privat information vill istället ha kontakt med vänner, familj och nya bekantskaper och väljer därmed nätverk som är mer inriktade på underhållning och bekantskapskretsar (Cutillo *et al.*, 2009).

Oavsett vilken information man väljer att dela med sig av så har nätverken en sak gemensamt; i skapandet av konto måste användaren acceptera användarvillkoren. Med i användarvillkoren brukar även integritetspolicyn ingå. Flinn och Lumsden (2005) menar att många användare tror att förekomsten av en sådan policy automatiskt betyder att nätverket lovar sekretess. Författarna menar också att så inte är fallet utan kan i själva verket innebära att nätverken kan frånsäga sig sekretessen. Användarna visade inte heller något stort förtroende för villkoren utan menade att de skrivs för att nätverken inte ska behöva ta ansvar (Flinn & Lumsden, 2005).

2.1.1 Applikationer inom sociala nätverk

Den ökade användningen av sociala nätverk har lett till att många av nätverken tillåter tredjeparts-applikationer för att höja upplevelsen användarna har av nätverken (Besmer, Richter Lipford, Shehab & Cheek, 2009). De spel, quiz, horoskop och andra funktioner som finns på Facebook [3] är alla exempel på tredjeparts-applikationer. Applikationerna tillåts att tillfoga information på användarnas profiler eller erbjuda användare nya aktiviteter. Med profil avses all information och loggar som varje användare har, där applikationerna främst använder sig av loggarna för att publicera vad användaren uppnår i applikationen, exempelvis när en ny nivå har nåtts i ett spel. De som anses vara populära applikationer är de som tillåter användare att spela spel och dela med sig av foton eller andra upplevelser som de haft tillsammans med bekanta (Besmer *et al., 2009).*

Flera av de sociala nätverken som använder sig av applikationer kräver att användaren skall godkänna applikationerna och deras krav före användning. Det kan innebära att applikationerna inte bara får tillgång till användarens information, utan även till den information som användaren har om sina vänner. Risken som följer är att applikationerna har tillgång till stor mängd data som användaren inte kan kontrollera när den används eller vilken information som samlas in (Besmer *et al.*, 2009; Krishnamurthy & Willis, 2008). Det är även möjligt för applikationen att samla in data om en användare som inte alls har godkänt applikationen, då en vän har samtyckt till

applikationens krav. Besmer *et al.* (2009) tar också upp approachen om allt-eller-inget som finns på vissa sociala nätverk, dvs att antingen så accepterar man applikationernas krav eller så kan man inte använda dem överhuvudtaget. Saltzer och Schroeder (1975) tar upp olika designprinciper, för vilka det genomgående temat är säkerhet och att ingen obehörig skall ta sig in i systemet. Approachen om allt-eller-inget för applikationer går direkt emot en av dessa designprinciper om minsta rättighet: att varje program och varje användare av systemet endast skall behöva hämta/lämna så mycket information som krävs för att slutföra arbetet.

Vid introduktionen av tredjeparts-applikationer på de sociala nätverken ökade trafiken ännu mer, bara den första veckan med dessa applikationer ökade trafiken på Facebook med 30% (Nazir, Raza & Chuah, 2008). I samband med att de sociala nätverken skapade utvecklingsplattformer för tredjeparts-applikationer ger nätverken möjligheten för både erfarna och oerfarna utvecklare att göra applikationer. Facebook är en av de största användarna av applikationer och trots den risk som utvecklingen av applikationerna kan ha till följd så är risken mindre än om de hade anlitat en extern webbapplikationsutvecklare då de genom en egen utvecklingsplattform kan ha mer kontroll över vad applikationerna får innehålla och vilken information som kan samlas in (Gjoka, Sirivianos, Markopoulou & Yang, 2008). Krishnamurthy och Willis (2008) påpekar dock att applikationer är en potentiell källa till informationsläckage, då de kan spåra användarens aktioner. Oron för säkerheten och privatlivet i applikationer förstärks än mer i sociala nätverk jämfört med andra distribuerade applikationer över Internet menar Cutillo *et al.* (2009), då de sociala nätverken har specifika sekretessfrågor till följd av deras hantering av personliga uppgifter. Till kategorin applikationer över Internet hör bland annat Wikipedia [6] och Google Calendar [7], men även webmail och online-auktioner hör hit.

2.2 Integritet

Integritet är ett vitt begrepp som kan definieras på flera olika sätt, och diskussionerna som pågår kring ämnet grundar sig på individuella rättigheter och skyldigheter. Om olika personer tillfrågas vad integritet är, skulle svaren troligtvis också skilja sig åt då det är ett väldigt känsligt ämne som man lägger in olika värderingar i. Integritet kan definieras som individens rätt att kontrollera sin personliga information, att den inte används utan individens tillåtelse men det kan också definieras som rätten att bli lämnad ifred, att inte bli personligt kränkt (Brodie *et al.,* 2005; Walters, 2001).

Under den snabba utvecklingen av IT de föregående decennierna fick begreppet integritet aldrig något större utrymme (Brodie *et al.,* 2009). Det fokuserades på att utveckla snabba, lättillgängliga sajter och att användaren skulle ha någon kontroll över informationen var ett mer underliggande mål. Det har dock skett en förändring inom området under 2000-talet, när allt fler organisationer använder system för att lagra information för att kunna utföra sina tjänster. Efter att rapporter om förseelser mot den personliga integriteten har frågan lyfts på nytt (Brodie *et al.*, 2005).

De lösningar till integritetsproblem som fanns förr är inte applicerbara idag, de är otillräckliga för de teknologiska framsteg som har gjorts (Walters, 2001). Förr var tanken att integriteten bevaras så länge informationen stannar inom lämplig kontext, idag kan det istället ses som att den personliga informationen får insamlas endast med användarens tillåtelse och för ett specifikt syfte och då endast för det syftet. Informationen får alltså inte bli publik eller säljas vidare utan användarens medgivande (Danezis, 2009). Även möjligheten att dölja information från systemet skall finnas enligt Cutillo *et al.* (2009) som också menar att all information skall enligt standardinställningarna vara gömt, så att användaren själv får ändra inställningarna ifall han/hon vill att de skall vara publika.

2.2.1 Användarbeteende

Användarbeteende är traditionellt sett hur användaren interagerar med systemet, baserat på användarens individuella egenskaper. Dock är de traditionella metoderna för att identifiera användarbeteende inte tillämpbara på sociala nätverk eftersom användare där interagerar både med själva sajten och med andra användare. Interaktionen sker genom uppladdning av innehåll på sajten och man kan se olika mönster i användarbeteendet för olika grupper av användare (Maia, Almeida & Almeida, 2008).

Som tidigare nämnts skapar användarna egna profiler som representerar dem, vilka kan ändras efter användarens egna önskningar. Ett socialt nätverk är ”only as good as the content their users share” (Burke, Marlow & Lento, 2009, s. 945), dvs att nätverket är direkt beroende av dess användare. Detta gör att nätverken dels uppmanar användare att bjuda in sina vänner, dels uppmanar användare att bidra med innehåll till nätverket. Användare börjar bidra med innehåll i samma stund som de skapar sina profiler och utvecklas sedan ju mer de är aktiva på nätverket, vilket gör att hela processen om hur användare beter sig på sociala nätverk är direkt avhängt till deras aktiviteter (Burke *et al.*, 2009; Squicciarini, Shehab & Paci, 2009).

Användarbeteendet skiljer sig avsevärt från det verkliga livet i avseendet vilka man anser vara sina vänner. På sociala nätverk blir användare vän både med dem som de känner närmare och dem som de knappt känner alls. Att vara vän med någon får således ett nytt begrepp, då användare generellt blir vänner med dem som är bekanta och som man inte direkt ogillar. Den information som då utlämnas på profilen visas även för de som användaren inte betraktar som närmare vänner och som informationen inte var avsedd för (Tufekci, 2008).

2.2.2 Uppgiftsutlämning

Användare avslöjar stora mängder information om sig själva på sociala nätverk, där även känslig information kan ingå, och de gör det utan att vara medvetna om de risker som det kan medföra. Vid profilskapandet och genom användandet av nätverket är utlämnande av information en ständig följeslagare. Hur mycket information som utlämnas kan variera från nätverk till nätverk, det kan vara mycket lite så som namn och lösenord, eller så kan det vara en stor mängd där mer ingående personlig information krävs. Hur mycket, hur känslig och vilka som kan komma åt

informationen som lämnas är däremot inte lika uppenbart för användarna, vilket gör att de kan lämna information som inte är lämplig i publik form (Schrammel *et al.*, 2009a; Squicciarini *et al.*, 2009).

Tufekci (2008) menar att de som lämnar ut information vill bli sedda och att detta är föga förvånande, men nämner också att det blir ett hot mot dem själva när de inte vet vem som kan se, vem som ser och vem som ser vad. Utlämningen av information ses som en nödvändighet av användarna för att de sociala nätverken skall vara användbara, för varför ska man ha en profil om den inte säger vem du är? Studier visar att när användare tillfrågats om risker för sociala nätverk har de antytt att de är medvetna om möjliga risker och att de tänker på sin integritet, men att det dock motsägs av hur användarna agerar då de snarare tänker på kort sikt istället för på vad som kan hända på lång sikt (Tufekci, 2008). Hur mycket information man lämnar ut har också en direkt koppling till hur många vänner du har, ju fler vänner desto mer utlämnad information (Flinn & Lumsden, 2005; Ross, Orr, Sisic, Arseneault, Simmering & Orr, 2009). Flera användare lämnar ut information som födelsedag, mobiltelefonnummer, adress, intressen, vilken skola man går på och vad ens politiska åsikt är. Vem som lämnar ut vad och vad som lämnas ut influeras av tre viktiga faktorer; framtida publik, kön och generell oro för den privata informationen (Gross & Acquisti, 2005; Young & Quan-Haase, 2009).

De sociala nätverken erbjuder vissa fördefinierade personliga inställningar när användaren skapar sin profil, inställningar som användaren i regel kan ändra när de vill. De fördefinierade inställningarna kan vara att all information skall vara tillgänglig för alla användare eller att endast vissa användare får tillgång till den personliga informationen. Ofta är standardinställningarna att alla användare kan få tillgång till all information och majoriteten av användarna ändrar inte dessa inställningar utan är nöjda med det skydd mot integriteten som inställningarna ger (Schrammel *et al*., 2009b).

2.2.3 Integritetshot

De sociala nätverkens uppmaningar till användarna att dela med sig av mycket information på sin profil gör att hoten mot den personliga integriteten ökar. Hoten är ofta av sådan karaktär att användaren inte tänker på dem när de skapar sin profil. Som definierat ovan så är integritet att användaren skall ha kontroll över sin information och att den endast får användas efter dennes tillåtelse och då endast för ett specifikt syfte. Hoten kommer inte bara från kriminella eller utomstående företag, utan de kan också komma från vänner och tredjeparts-applikationer (Cutillo *et al.*,2009; Krishnamurthy & Willis, 2008).

Säljande av information

Ett vanligt sätt att få tillgång till potentiella kunder är för marknadsförare att samla in mail-adresser från olika serverlistor, chattrum osv. Förändringen med de sociala nätverken är att marknadsförarna då kan få tillgång till information i realtid med hjälp av användaren själv. Det har diskuterats huruvida det är etiskt riktigt av företagen som vill åt informationen att göra på detta sätt, men i vissa fall är det nätverken själva som förser företagen med informationen. Den

information som de kräver när användaren skapar en profil är till stor del för att kunna förbättra servicen och standarden på nätverket, men det finns fall då nätverken har sålt information utan användarens vetskap, vilket kan leda till oönskad mail, telefonsamtal etc. (Chen & Shi, 2009).

Informationen som användarna tillhandahåller nätverken lagras på servrar och även om användaren avslutar sitt konto på nätverket så finns deras information kvar. Det gör att nätverken får ett värde på marknaden som höjs ju fler användare nätverket har, och när nätverket säljs följer all information med till den nya ägaren (Cutillo *et al.*, 2009).

Förföljelse och direkt skada

Den information som tillhandahålls på de sociala nätverken kan leda till förföljelse både online och offline. Genom användarens profil och statusuppdatering avslöjas var han/hon befinner sig stora delar av dagen och information om bostad, schema etc. kan också avslöjas. Detta gör det möjligt för en potentiell förföljare att avgöra inte bara var användaren befinner sig utan också vad användaren gör för tillfället (Gross & Acquisti, 2005).

Informationen som förföljare kan använda sig av kan också användas av personer som använder den till förtal eller till att personifiera en användare, vilket får en direkt påverkan och skada på de inblandade parterna (Cutillo *et al.*, 2009). Utpressning är en form av direkt skada och kan uppstå av att användaren finns med på bilder eller har lagt ut kommentarer som när de tas ur sitt sammanhang blir direkt olämpliga. Spannet för utpressning, direkt skada och förföljelse kan vara allt från genans och förlägenhet till diskriminering (Anderson, Bonneau, Diaz & Stajano, 2009; Gross & Acquisti, 2005).

Identifiering

Även om den information som användaren lämnar ut på ett nätverk inte är tillräckligt för att identifiera användaren, så kan angripare få en bra uppfattning och identifiera användaren om denne har konton på flera olika nätverk. Den information som lämnas ut är ofta likartad även om viss information skiljer sig, och med hjälp av detta kan angripare bilda sig en uppfattning om användaren. Användare har ofta samma profilnamn eller profilbild på sina olika konton vilket möjliggör bland annat ansiktsidentifikation, att kunna koppla två till synes helt skilda konton till varandra. Det är också möjligt att länka två konton till varandra baserat på den demografiska information som ges (Cutillo *et al.*, 2009; Gross & Acquisti, 2005).

Att bli identifierad innebär att integriteten minskar avsevärt och att även anonym information avslöjas. Identifieringen kan i ett senare skede leda till stulen identitet och utpressning (Gross & Acquisti, 2005; Strater & Richter Lipford, 2008).

2.3 Säkerhet

Integritet har ovan definierats som rätten att kontrollera sin personliga information. Säkerhet å andra sidan rör de tekniker som kontrollerar vem som kan använda eller ändra informationen. Säkerhetsdelen av ett förlopp är inte användarens mål utan snarare en deluppgift för att komma till målet, till exempel genom login till de sociala nätverken. Även om det inte är själva målet för användaren så ska säkerhetsdelen av ett förlopp innebära att den personliga integriteten skyddas (Chiasson, Forget, Stobert, van Oorschot & Biddle, 2009; Saltzer & Schroeder, 1975).

Den omedvetenhet som användare har gällande vad den information de lämnar ut används till innebär inte bara vissa integritetshot utan även vissa säkerhetsrisker. Den kriminella aktiviteten på Internet söker sig dit det finns värdefull information och nätverk där säkerhetsprogram används utgör en potentiell källa. Det finns olika sätt för kriminella att samla den information de behöver, där ett sätt är att utnyttja användarens tillit till nätverk och andra användare. Användaren är på grund av detta den svagaste länken i ett socialt nätverk, sett ur ett säkerhetsperspektiv (Bilge, Strufe, Balzarotti & Kirda, 2009; Chiasson *et al.,* 2009).

Säkerhetsrisker kan uppstå när programmeringen är dåligt utförd, dvs att buggar eller luckor i behandlingen av information existerar. Det finns också en paradox i säkerhet och användande då designutformandet av säkerheten kan innebära att användbarheten förbättras men säkerheten försämras. Om den försämrade säkerheten då skulle korrigeras kan det leda till att systemet blir oanvändbart eftersom användarna då kommer att försöka kringgå eller missbruka säkerhetsmekanismerna (Chiasson *et al.,* 2009).

Det är inte bara i systemet och systemutvecklingen som säkerhetsrisker kan uppstå utan även i hur användaren ser på säkerhetssystemet. Användaren har ofta en alltför stor tillit till systemet och är inte medveten om de risker som finns och luras relativt enkelt till att delge information till obehöriga. Även de användare som har ett mer skeptiskt förhållningssätt kan luras till att delge information genom till exempel social engineering och phishing (Bilge *et al.,* 2009).

2.3.1 Lösenordsgenerering

Att hitta ett nätverk eller en funktion där användaren har ett konto utan att ett lösenord krävs för inloggning är i stort sett omöjligt. Lösenord används överallt, till mail, chatt, sociala nätverk osv. När användare ska välja lösenord har de en tendens att välja lösenord som är relativt enkla att gissa och många återanvänder dessutom samma lösenord på olika konton, då de har problem med att minnas flera lösenord (Chiasson *et al.,* 2009; Florêncio & Herley, 2007; Mark, Lomas, Gong, Saltzer & Needham, 1989).

Varje system där användaren skall registrera ett lösenord har olika krav på lösenordet; vissa låter användaren välja helt själv, vissa kräver ett antal tecken, vissa genererar lösenord åt användaren. De gånger systemet tvingar användaren att ha ett genererat lösenord eller har vissa krav på

lösenordet kan det skapa ett motstånd hos användaren. När användaren själv får välja lösenord väljer de ofta något som de har en relation till för att det ska vara lätt att komma ihåg. Användningen av relationer i ett lösenord, tillsammans med faktumet att samma lösenord återanvänds, gör att användarnas lösenord ofta är lätta att gissa sig till. Speciellt utsatta är användarna om inloggningsfunktionen inte har någon varningsfunktion vid flertalet misslyckade inloggningsförsök (Florêncio & Herley, 2007; Kuo, Romanosky & Cranor, 2006; Mark *et al.*, 1989; van Oorschot & Thorpe, 2008).

Lösenord används för att skydda konton med värdefulla uppgifter och det gör att de är attraktiva för kriminella attacker. Återanvändandet av lösenord gör då att sårbarheten i lösenordet ökar eftersom en angripare kan få tillgång till flertalet konton om de knäcker ett lösenord. Angripare kan till exempel använda sig av phishing eller sabotageprogram för att ta reda på användares lösenord. Problemet med användare som har för lätta lösenord har fått sällskap av problemet med användare som ovetande avslöjar sina lösenord öppet (Florêncio & Herley, 2007; Gaw & Felten, 2006).

2.3.2 Säkerhetshot

Till skillnad från integritetshoten som kan komma från både kriminella, företag och andra användare så kommer säkerhetshoten främst från de kriminella. Utvecklingen med sociala nätverk har öppnat nya möjligheter för de kriminella och det är inte längre endast hot mot system som existerar, utan det finns även hot som inriktar sig mot användaren för att få tillgång till information (Bilge *et al.*, 2009; Joinson, 2008).

Social Engineering

Social engineering är ett hot som innebär att offret blir lurad att lämna ut känslig information ovetande om att han/hon lämnar den till en obehörig person. Det finns många olika sätt att utföra dessa attacker. Ett exempel är att utge sig för att vara en person som är högre i hierarkin i företaget där offret jobbar och därigenom få personen att lämna ut information. Anledningen till att social engineering används är att användaren ses som den svagaste länken i ett företags säkerhetslösning då det inte går att påverka vad användaren ger ut för information (Orgill, Romney, Bailey & Orgill, 2004; Whitman & Mattord, 2005).

Vid social engineering använder angriparna manipulation och känslor för att få information från användarna. Det går att identifiera fyra angreppssätt; vårdslöshet, bekvämlighet, hjälpsamhet och rädsla. Beroende på vad angriparen vill ha för information tar denne på sig olika roller för att uppnå känslorna och därmed få tillgång till informationen (Orgill *et al.*, 2004; Twitchell, 2006).

Phishing

Phishing är ett hot där angriparen utger sig för att vara ett pålitligt företag för att kunna använda sig av social engineering och få användare att klicka på en länk. Phishing kan ta många uttryck, det kan förekomma på sociala nätverk, via mail eller på andra webbplatser. Det kan också innefatta delar av användarens webbläsare genom att dölja varningar på vissa sidor. Angriparna

som använder sig av phishing är intresserade av identitetsstöld och försöker komma åt information som de kan använda genom att till exempel uppmana människor att kontrollera sin kontoinformation. Ett annat sätt att få tillgång till informationen är att be folk delta i en undersökning där dels personliga uppgifter efterfrågas, dels uppmaning att lämna bankkontonumret för att kunna få ersättning ges (Chen & Shi, 2009; Kumaraguru, Rhee, Acquisti, Cranor, Hong & Nunge, 2007; Luo *et al.*, 2009).

För tillfället är det fortfarande vanligast med phishing över mail och det är en process som fortfarande är i utvecklingsstadiet för de kriminella, mailen som skickas blir alltmer sofistikerade och svåra att identifiera vilket även leder till att ”äkta” webbplatsers råd och förfrågningar ifrågasätts. Det finns en stor omedvetenhet bland användare men trots den medvetenhet som finns när användarna vet hur attackerna ska identifieras faller ett stort antal ändå för dem (Kumaraguru *et al.*, 2007).

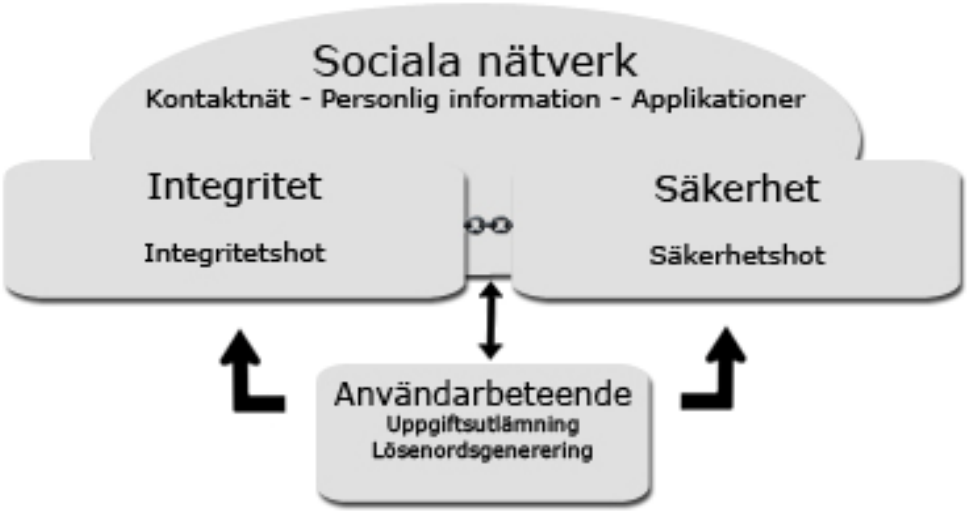
Data mining
Data mining innebär att angriparen lägger ihop fragment av användares information. Den bild som angriparen får fram kan, med tillräckligt många fragment, vara en hel personakt. Genom att samla fragment av tillgänglig information kan angriparen till och med ta reda på personnummer eller kontonummer. Grundidén i data mining är att upptäcka dolda mönster från insamlad data (Chen & Shi, 2009).

Det pågår diskussioner kring huruvida data mining är lagligt eller ej, då informationen som analyseras kan ha inhämtats på laglig väg, det vill säga den har varit tillgänglig på sociala nätverk etc (Chen & Shi, 2009; Kantarcioglu, Jin & Clifton, 2004).

2.4 Begreppssammanfattning / Teorisammanfattning
Nedan illustreras vårt teoretiska ramverk i form av hur vi kopplar samman de beskrivna områdena ovan (se figur 2.1).

Vårt perspektiv utgår från de sociala nätverken då det är de som är vår undersökningsplattform. De sociala nätverken innebär för användare vissa risker gällande integritet och säkerhet. Dessa två är sammankopplade med varandra eftersom de påverkar varandra. Säkerheten på ett socialt nätverk har påverkan på hur integriteten skyddas och de integritetshot samt säkerhetshot som finns flyter ofta in i varandra och är svåra att separera.

Yttre faktorer där användaren står i fokus påverkar huruvida integriteten kan skyddas av de sociala nätverken eller ej. Användaren har även ett stort inflytande i säkerheten för sitt eget konto då t ex användaren själv väljer lösenord. Samtidigt påverkas användaren av de insinuationer som det sociala nätverket ger.



Figur 2.1 Begreppssammanfattning

3 Metod

I detta kapitel beskrivs tillvägagångssättet för datainsamling i form av teori- och empiriska studier. Inledningen består av valet av metod och ansats och efterföljs av hur litteraturstudierna och datainsamlingen har utförts. Vidare behandlas analys av data samt metodkritik.

3.1 Val av metodansats

Hur verkligheten ser ut är inte klart definierat men hur den tolkas kan forskaren ta fram genom att undersöka människors reflektioner av den. I forskning kan datainsamlingen innehålla två olika typer av ansatser; kvalitativa och kvantitativa (Backman, 1998). Den kvalitativa ansatsen innebär att undersöka på djupet, där känslor och upplevelser kan spela stor roll, till skillnad från den kvantitativa ansatsen som går mer på bredd än på djup (Jacobsen, 2002). Den kvantitativa studien använder siffror som den centrala analysenheten, eftersom man vill mäta företeelser som sedan kan översättas till dessa siffror. När det är gjort används olika statistiska metoder för att analysera insamlad data (Denscombe, 2000). Jacobsen (2002) menar att båda ansatserna är bra på olika sätt och används i olika sammanhang och problemställningar och Kvale (1997) understödjer detta när han skriver att metoden väljs utifrån vilka forskningsfrågor som skall ställas.

Syftet med undersökningen var att få insikt i vilken inställning användare har till integritetsfrågor samt vilken medvetenhet de har om säkerhetsrisker. Detta syfte är en del av det underlag som krävs för att nå målet för uppsatsen, hur användaren kan vidta försiktighetsåtgärder för att skydda sig. För att kunna nå vårt mål behövde vi få en bred kunskap om hur användare upplever sin inställning och sitt beteende snarare än en djup kunskap om fåtalet individer. De försiktighetsåtgärder som skall läggas fram ska kunna vara tillämpbara för alla användare vid ett nätverk och därmed krävdes också ett större urval av respondenter för att få ett representativt urval. Vi valde därför att använda oss av en kvantitativ ansats då Jacobsen (2002) argumenterar för att den går mer på bredd än på djup. Dessutom ville vi mäta företeelser för att sedan kunna analysera dem och kunna ta fram statistisk data, vilket överensstämmer med hur den kvantitativa metoden används enligt Denscombe (2000). Statistiken och analysen kom att ligga till grund för hur vi utformade våra rekommendationer.

Undersökningen genomfördes i två delar; den första delen var att kartlägga vad tre olika sociala nätverk har för inställningar och funktioner som kan innebära säkerhets- och integritetshot för användaren. Den andra delen av undersökningen genomfördes i de tre sociala nätverken som redan kartlagts, där webbenkäter skickades ut/lades upp som länk för att undersöka inställning, medvetenhet och beteende till integritets- och säkerhetsfrågor. Frågorna till webbenkäten utgick från en operationalisering av begreppen sociala nätverk, integritet och säkerhet. Utifrån enkätsvaren kunde vi analysera användares inställning och medvetenhet i jämförelse med deras påstådda beteende. Då vi endast har ifrågasatt användares beteende i enkät och inte har använt oss av några observationer är vi medvetna om att validiteten i vissa av dessa svar kan frångå det

faktiska beteendet, men tycker att det är intressant att undersöka även med dessa risker. Analysresultatet användes sedan tillsammans med resultatet från kartläggningen för att kunna ge rekommendationer till användare angående hur man kan vidta försiktighetsåtgärder på sociala nätverk.

3.2 Litteraturstudier

Den teoretiska referensram vi har byggt upp har hämtat material från vetenskapliga artiklar och litteratur som är relevant för ämnesområdet. Det inhämtade materialet berör områden så som sociala nätverk, integritet och säkerhet. De vetenskapliga artiklarna som har använts har inhämtats via databaserna ACM och IEEE. Nyckelord som användes som sökord var: privacy, integrity, security, social networks och password.

3.3 Datainsamling

Datainsamlingen består av ett antal moment som skall ligga till grund för den avslutande diskussionen mot slutet av uppsatsen.

3.3.1 Kartläggning av valda sociala nätverk

I enlighet med vårt första syfte som var att kartlägga vilka funktioner och aktiviteter som kan innebära ett hot mot användarens integritet och säkerhet på sociala nätverk, var det av vikt att undersöka dessa områden på de tre sociala nätverk som valts ut till vår kvantitativa studie. Arbetet gick tillväga på så sätt att vi undersökte de sociala nätverkens efterfrågan av information vid profilskapande samt deras standardinställningar för att sedan jämföra dessa resultat med den teoretiska referensramen. Vi kunde därefter kartlägga vilka funktioner och aktiviteter som är potentiella hot mot användaren och dennes integritet och säkerhet.

Facebook blev ett av valen med tanke på den stora spridning nätverket har både geografiskt och demografiskt, med över 400 miljoner användare i mer än 180 länder [4]. Ett annat socialt nätverk som vi valde är match.com som är en datingsajt för svenska singlar. Match.com har en stor andel av de användare som idag använder sig av dating på Internet inom Sverige. Det tredje och sista sociala nätverket vi valde att skicka ut enkäterna till var på Twitter, vilket är en form av miniblogg. Att just dessa tre nätverk valdes har sin grund i att vi ville täcka upp ett större område av de olika kategorier som finns i sociala nätverk, där de olika sajterna täcker upp kategorierna gemensamma intressen, vänner samt dating (Gross & Acquisti, 2005). Kvale (1997) nämner att respondenterna skall väljas efter vilka resurser som finns representerade och för att kunna få en större representation valde vi att använda oss av tre nätverk som har olika mål.

För vart och ett av de tre nätverk som vi har valt att studera närmare undersökte vi vilken information som krävdes vid skapandet av en profil. Vi kunde här kartlägga vilka uppgifter som var obligatoriska och vilka som var frivilliga, samt hur tydligt dessa alternativ var markerade. Redan på detta stadium ville vi också kartlägga huruvida man direkt kunde ändra sina säkerhetsinställningar eller ej. Efter profilskapandet undersökte vi också hur användaren kan välja att ändra sina inställningar och vad som visas på profilen, samt ifall det fanns olika

valmöjligheter gällande olika sorters information. Efter avslutad kartläggning av nätverken jämförde vi resultatet med vår teoretiska referensram för att sammanställa de hot mot integriteten och säkerheten som finns på sociala nätverk.

Kartläggningen gav oss en viktig grund för att kunna svara på vår fråga om hur användare kan vidta försiktighetsåtgärder då vi mer specifikt kan ge rekommendationer för varje nätverk när vi är medvetna om hur dessa nätverk är utformade. Den här delen av studien utfördes efter enkäten var utformad och utskickad/upplagd, då vi ansåg att den inte skulle innebära någon förändring i de frågor vi ställde i enkäten. Hade kartläggningen utförts innan enkäten konstruerades så hade den kunnat ligga till grund i vissa frågor i enkäten men vi ville inte ha någon påverkan som kunde ha uppkommit i samband med kartläggningen vid enkätsammansättningen.

3.3.2 Val av datainsamlingsmetod

Svarsinsamling kan ske på ett antal olika sätt när en kvantitativ undersökning utförs; genom post-enkäter, telefonintervjuer eller standardiserade besöksintervjuer, där post-distributionen var den vanligaste metoden (Jacobsen, 2002). Författaren menar att post-enkät lämpar sig bäst när undersökningen kräver låga kostnader och ringa intervjuareffekt. Vilken metod man använder baseras också på vilken grupp som undersöks, dvs urvalet.

Med Internets expanderande har även webbenkäter blivit ett allt vanligare fenomen där respondenten dessutom kan erbjudas interaktion på ett nytt sätt med hjälp av ljud och bilder och fortfarande ha kvar sin anonymitet (Couper, Tourangeau & Steiger, 2001). Webbenkäter tillåter forskaren att komma i kontakt med och få svar av respondenter via Internet vilket innebär att lämpliga respondenter som hade varit utom räckvidd vid en post-enkät kan nås i en webbenkät.

Vi valde att utföra webbenkät av fyra anledningar.

1. Kostnader. Det innebar en lägre kostnad då vi inte behövde trycka upp enkäterna och skicka dem via post till respondenterna.

2. Snabbhet. Vi hade svaren direkt efter att respondenten svarat och behövde inte vänta på att enkäterna skulle skickas tillbaka.

3. Urvalet. Detta hänger ihop med både kostnad och tid. För att få tag på respondenterna hade vi varit tvungna att söka upp dem fysiskt för att skicka enkäterna via post vilket vi inte behövde göra med enkäter via webben. Vi ville också få kontakt med respondenterna där de är användare, dvs på de sociala nätverken.

4. Anonymitet. Vi kunde garantera att respondenterna var helt anonyma i sitt svar vilket kan resultera i en högre svarsfrekvens (Jacobsen, 2002).

Det som däremot kan bli lidande av att utföra en onlineundersökning är svarsprocenten. Det är lättare att ignorera en länk som skickas än ett fysiskt brev. Detta försökte vi i viss mån kompensera för genom att garantera anonymitet.

3.3.3 Urval av respondenter

När en empirisk studie utförs behöver forskaren hitta ett antal respondenter som svarar på dennes frågor angående det studerade ämnet. Detta kallas för att göra ett urval och görs för att begränsa antalet människor som svara för att få en hanterbar mängd intervjuer eller enkäter. Det skulle helt enkelt bli för dyrt och ta för lång tid att låta alla relevanta respondenter svara på forskningsfrågorna (Trost, 2001). Urvalstyper brukar delas in i två olika kategorier: slumpmässiga- och icke slumpmässiga urval. Antalet respondenter är beroende av vad som skall undersökas (Kvale, 1997) och skall väljas efter vilka resurser som finns representerade hos forskningsobjektet.

Utifrån vårt perspektiv där användare av sociala nätverk står i fokus valde vi först att göra en tydlig avgränsning i antalet sociala nätverk samt vilka sociala nätverk undersökningen skulle genomföras på. Detta för att kunna koncentrera oss på få specifika nätverk där försiktighetsprinciper kan ges för nätverket istället för att ge generella principer som inte kan användas på alla sociala nätverk med tanke på olika förutsättningar. I urvalet av vilka sociala nätverk som skulle ingå i studien valde vi att använda oss av en icke-slumpmässig metod (Trost, 2001) för att få en större representation bland nätverken.

Efter det första urvalet med vilka nätverk som skulle ingå i studien skulle ytterligare ett urval göras som berörde vilka respondenter inom de respektive nätverken vi skulle rikta oss till.

Tidigare nämndes två olika kategorier av urval: slumpmässiga och icke-slumpmässiga. De olika urvalsmetoderna lämpar sig till olika former av undersökningar, där obundna slumpmässiga urval är en form av slumpmässigt urval. Obundna slumpmässiga urval innebär att inget annat än slumpen avgör, till skillnad från bundna slumpmässiga urval där urvalet härrör sig till vissa bestämda punkter men som utöver det är slumpmässigt (Trost, 2001).

Vi valde att använda oss av bundna slumpmässiga urval då vi själva begränsades till viss del av de sociala nätverken och ansåg att det innebar svårigheter att nå ut till respondenter som var helt slumpmässigt utvalda på det sätt som Trost (2001) anser att det urvalet skall vara.

Urvalsmetoden resulterade i att i de nätverk vi inte redan hade kontakter (match.com, Twitter) valde vi att skapa konton för att sedan via nyfunna vänner skicka ut enkäten. Vännerna hade vi tagit kontakt med via nätverken och förklarat vår studie och varför vi ville ha kontakt. På Twitter valde vi att lägga upp en länk, då vänner inte förekommer på samma sätt i Twitter som i många andra nätverk. Gällande Facebook ville vi inte att det skulle bli ett bekvämlighetsurval och försökte därför istället att nå respondenter via nätverk och då genom att skicka ut enkäten till enskilda användare. Begreppet ”nätverk” när det gäller Facebook är ett område som definieras

som nätverk, t ex Halmstad eller Sverige. Vi valde att skicka ut enkäten till personer i nätverket Sverige.

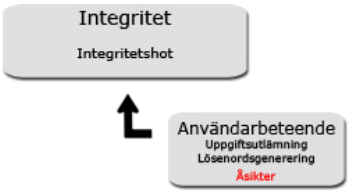
Utskicket på Facebook resulterade i att 140 respondenter uppmanades att svara på enkäten. På Twitter lade vi upp en länk och det är därför svårt att uppskatta hur många respondenter som har haft tillgång till länken. De respondenter vi var i kontakt med på match.com fick en kort förklaring av projektet samt länken till enkäten. Då vi var tvungna att söka upp varje respondent enskilt resulterade antalet tillfrågade respondenter i 30 st. Totalt kan vi konstatera att det var 170 respondenter som enkäten skickades ut till och utöver det ett mörkertal på hur många som har haft tillgång till länken via Twitter.

Enkäten fanns tillgänglig i en vecka och under den tiden skickades det även ut påminnelser till de respondenter som vi hade tagit kontakt med. Svarsfrekvensen räknat på de utskickade enkäterna blev strax över 50%, 92 st. Efter radering av 15 st ogiltiga svar blev svarsfrekvensen 77 st, 45%.

3.3.4 Operationalisering av begrepp

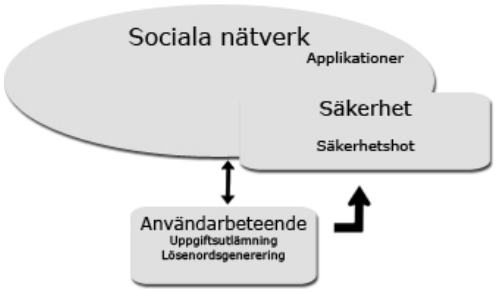
Operationalisering är ett sätt att konkretisera de begrepp som är centrala för att kunna göra dem mätbara (Jacobsen, 2002). Då de centrala begreppen ofta är vaga och kan tolkas på flera sätt måste en operationalisering av dem ske, där en indirekt mätning sker då begreppen ges ett eller flera värden som är subjektivt utvalda av forskaren. Ibland är det inte tillräckligt med att konkretisera begreppet en gång utan det krävs en fortsättning som kan pågå i flera nivåer. Operationaliseringen är en lång process som ofta börjar i ett vagt begrepp för att sluta när det finns ett starkt underlag till vilka frågor som ska finnas med i den kvantitativa studien (Jacobsen, 2002).

Första steget i vår operationalisering innebar att bryta isär vår problemformulering och syften för att få ett antal olika begrepp som vi ville mäta. Huvudkategorierna som mättes blev då *Integritet* och *Säkerhet*. Då vi ville mäta användares inställning till integritet delade vi även upp den kategorin i två underkategorier: *Åsikt* och *Beteende*. Dessa behandlar hur användaren tänker respektive handlar i givna situationer. För att få en tydligare bild av vilka frågor enkäten skulle innehålla delades underkategorierna upp i fyra interaktioner användaren kan delta i på nätverken. *Profilskapande* som behandlar skapandet av användarkontot och uppbyggnad av profil, *Inställningar* som behandlar vilka val användaren kan göra för att manipulera sin profil, *Interaktionsparter* som behandlar vem användaren interagerar med och slutligen *Interaktionstyper* som behandlar de typer av interaktion användaren kan ställas inför. De fyra interaktionerna fick sedan ett antal påståenden knutna till sig som behandlar respektive område utifrån den teoretiska referensramen. Var interaktionsfrågorna integreras i figur 2.1 visas i figur 3.1.



Figur 3.1 Operationalisering integritet

Säkerhet i sin tur operationaliserades utefter användarens medvetenhet om säkerhetsrisker. De teman som bearbetades här är *Lösenord*, *Säkerhetshot* och i de fall där nätverket tillåter *Applikationer*. Även dessa teman fick sedan ett antal mätbara påståenden knutna till sig. Hur säkerhetsfrågorna appliceras och hör ihop med resterande begrepp visas i figur 3.2.



Figur 3.2 Operationalisering säkerhet

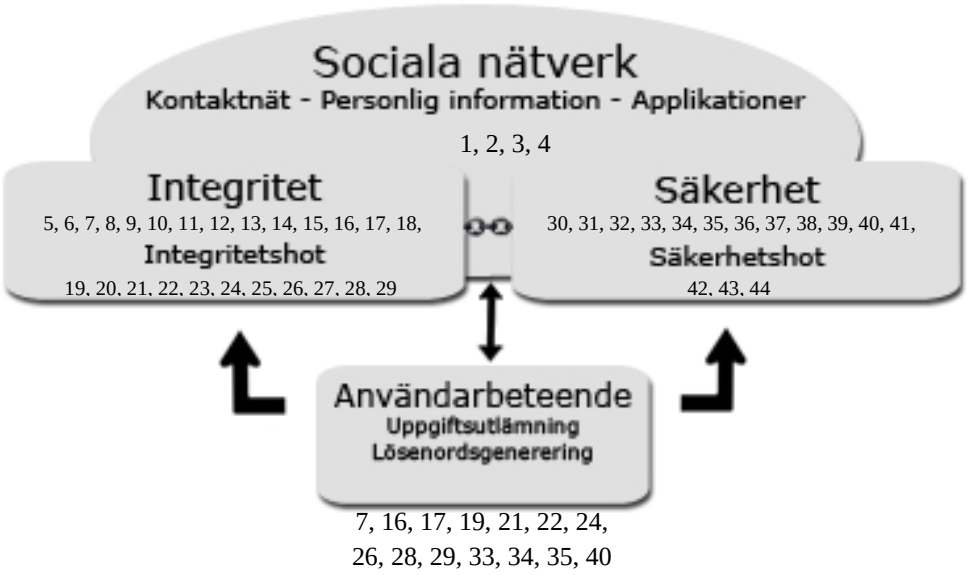
Vi valde att operationalisera våra centrala begrepp i dessa teman och kategorier då vi ville få en uppfattning både om hur användarnas inställning till integritetsfrågor är och hur användarna menar att de faktiskt agerar när de interagerar på de sociala nätverken. Det var viktigt att undersökningen omfattade båda delarna så att analysen av dessa kunde ligga till grund när försiktighetsåtgärderna och rekommendationerna skulle arbetas fram, se figur 3.3.

Integritet			
Beteende			
Profilskapande	*Inställningar*	*Interaktionsparter*	*Interaktionstyper*
Inställningen till hur integriteten påtänks vid skapande av profil.	Inställningen till vilken information användaren vill visa.	Vilka andra parter användaren vill dela sin information med.	Användarens inställning till de olika interaktionstyper som erbjuds.
Jag är mån om min personliga integritet när jag skapar nya användarkonton.	Jag är rädd att nätverken skall använda min information på ett sätt som gör att jag blir utlämnad.	Jag litar på att de vänner jag lägger till inte kommer att lägga ut olämplig information om mig.	Jag litar på att nätverken inte använder min information utan min tillåtelse.

Figur 3.3 Urklipp av operationaliseringsschema. Hela operationaliseringsschemat återses i Bilaga 1.

Som vårt andra syfte presenterar så skulle vi, utöver att undersöka inställning till integritet och påstådda beteende, även undersöka medvetenheten om säkerhetsrisker på sociala nätverk och valde därför att göra en undersökning som innefattar säkerhetshot, lösenord och applikationer. Alla dessa tre teman utgör en grund i de säkerhetshot som kan uppstå och som kan påverka den personliga integriteten.

Resultatet av operationaliseringen blev de frågor som sedan utgjorde webbenkäten. Figur 3.4 nedan visar hur de olika frågorna hör ihop med de olika begrepp som har operationaliserats (se bilaga 2a).



Figur 3.4 Enkätfrågor i relation till begreppsbilden

3.3.5 Enkätens utformning

När enkätfrågor utformas måste forskaren dels tänka på hur frågeställningen formuleras, dels hur svarsalternativen utformas.

Vid formulering av frågeställningar finns det ett antal tumregler som bör finnas i åtanke. Sammanfattat skall man tänka på att eftersträva enkelhet i frågorna, definiera begrepp, undvika ledande frågor, undvika känsliga frågor och variera frågornas riktning (Jacobsen, 2002). Reglerna syftar till att hålla enkäten objektiv och saklig, och låta respondenten själv ta ställning till de frågor eller påståenden som ställs.

Frågornas utseende varierar efter vad undersökningen syftar till att mäta. Dels finns det olika frågekategorier, där kunskapsfrågor och frågor om attityder och åsikter finns med och används när kunskap om ett fenomen respektive när inställning till ett fenomen ska undersökas. Den andra delen är att frågorna kan skrivas antingen som direkta frågor som skall besvaras eller som påståenden som respondenten skall ta ställning till (Jacobsen, 2002).

Svarsalternativ kan delas in i tre olika typer av svar: kategorisvar, rangordnade svar och metriska svar (Jacobsen, 2002). Kategorisvar syftar till att ge respondenten tydliga svarsalternativ att välja

mellan. Det kan till exempel handla om att fråga vilket kön respondenten har då svarsalternativen kvinna och man ges. Rangordnade svar handlar om att mäta intensiteten i ett påstående medan svar av metrisk natur har ett värde i form av siffror, som t ex vid angivande av ålder.

Vilket spann som ska användas vid svarsalternativ för rangordnade svar är inte självskrivet (Jacobsen 2002). Antalet svarsreferenser kan variera, att ha fyra-fem val är det vanligaste. Ofta används fem val när man vill ge respondenten möjligheten att välja ett neutralt alternativ, mittenalternativet, som också kan fungera som ett ”vet ej”-alternativ. Fyra val kan användas när man vill tvinga respondenten att ta ställning i en fråga. Båda alternativen har sina för- och nackdelar, och vilket alternativ som passar bäst för studien är upp till forskaren att bedöma (Jacobsen, 2002). Att ha fem val i en åsiktsfråga där svaren är utformade som ”instämmer helt (1) – instämmer inte alls (5)” kallas för en Likertskala, där de som har svarat t ex ”2” (instämmer delvis) kan ses som mer positiva än de som har svarat 3-5 (Denscombe, 2000).

För att kunna mäta användarnas inställning till integritetsfrågor och medvetenhet om säkerhetsrisker valde vi att ha med både kunskapsfrågor och attityd/åsiktsfrågor. En attitydfråga kan t ex vara *”Hur känner du inför att gå i en mörk grotta?”* och en kunskapsfråga kan vara *”Vad är farligast vid bilkörning?”*. I båda fallen har respondenten förprogrammerade svar där de antingen ska ta ställning eller ska välja det alternativ som passar bäst in på dem. De frågor som rörde integriteten, både inställning och beteende, konstruerades till attitydfrågor, medan de frågor som rörde medvetenheten om säkerhet formulerades till kunskapsfrågor. Detta medför att även svarsalternativen för de olika frågorna blev olika, vilket vi återkommer till.

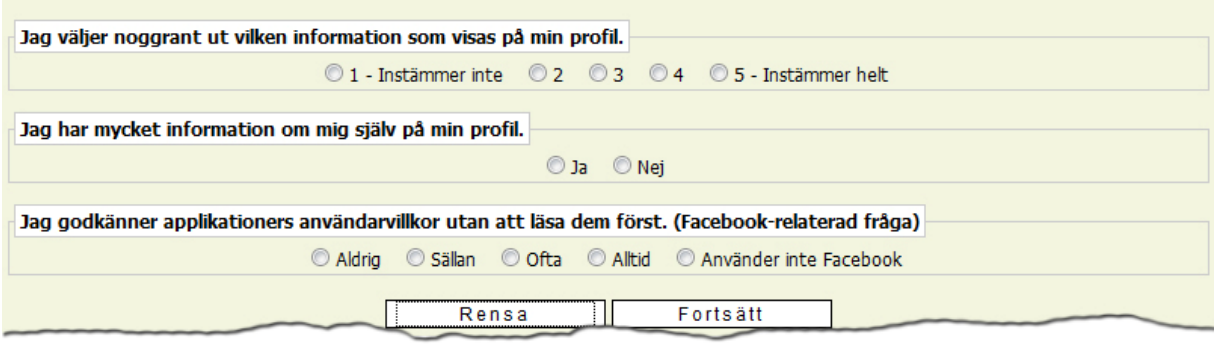
Vi valde också att ha en majoritet av påståendefrågor istället för direkta frågor, då vi ville att respondenten skulle ta ställning till det som frågades istället för att svara på givna alternativ. Påståendefrågorna gav oss också en större möjlighet att analysera respondenternas inställning till integritet och säkerhet med det spann som gavs som svarsalternativ. Respondenten kan välja att förhålla sig neutral (3) till frågan eller visa att de instämmer/inte instämmer (2/4) utan att behöva instämma helt/inte alls (1/5). Detta gav respondenten en större möjlighet att nyansera sitt svar.

Vid utformningen av frågorna tog vi hänsyn till de tumregler som Jacobsen (2002) tog upp. Frågorna gjordes så korta och med så enkelt språk som möjligt för att kunna tillmötesgå alla potentiella respondenter. De begrepp vi identifierade som möjliga problembegrepp då de kan tolkas på olika sätt, valde vi att tydligare förklara och definiera i inledningen till enkäten. Flera frågor har värderingar i sig eftersom respondenten ska kunna ta ställning till frågan, vilket kan göra att frågorna blir ledande, dock har vi i de fallen valt att även ha frågor som är motsvarande i andra riktningen.

Vi har i vår enkät använt rangordnade svar för att mäta frekvens av en aktivitet hos användaren och hans/hennes åsikt om integritet på sociala nätverk. Metriska svarsalternativ har använts där vi frågar om respondentens ålder. Vilket spann som har använts vid de rangordnade svaren har varit varierande beroende på vilken fråga som ställts. Vi har använt oss av två olika spann;

instämmer helt – instämmer inte alls; samt aldrig – alltid. Alternativen ”helt-delvis-inte alls” finns också med vid vissa frågor och utöver det har vi också använt oss av ja/nej-frågor gällande kunskapsfrågorna för att där följa upp med en öppen fråga. De olika svarsalternativen är utarbetade efter vilken fråga som har ställts, då påståenden som ”Jag läser alltid användarvillkoren först” inte är kompatibel med ”instämmer helt – instämmer inte alls” utan snarare ska refereras till hur ofta användaren läser användarvillkoren.

När olika svarsalternativ har använts så har vi använt oss av olika många val i svaret. Vid alla ”instämmer”-svar kan respondenten svara på en Likertskala med fem svarsalternativ för att ge respondenten möjligheten att vara neutralt. Däremot valde vi i tidsfrågorna att bara använda oss av 4-gradig skala, då responden dels tvingas ta ett beslut, dels täcktes de relevanta tidsspannen in i de fyra alternativen; aldrig, ibland, ofta och alltid, se figur 3.5.



Figur 3.5 Urklipp från enkät. För hela enkäten, se Bilaga 2.

Innan enkäten distribuerades till respondenter vid de olika nätverken gjorde vi ett pilottest av enkäten. Pilottestet utfördes för att testa funktionalitet av enkäten samt förståelse för frågor och svar i enkäten. Testet tillät oss upptäcka eventuella fel och medförde att vi kunde ändra dessa innan enkäten distribuerades till våra respondenter. Pilottestet genomfördes på fem respondenter som alla var användare av sociala nätverk och därmed representativa för vårt urval. Detta medförde att även dessa respondenters svar finns med i det resultat som presenteras i avsnitt 4. När pilottestet var genomfört och det fel vi upptäckte var åtgärdat distribuerades enkäten på de tre nätverken. De förändringar som genomfördes efter pilottestet var redaktionella språkliga ändringar varvid pilottestresultaten fortfarande var giltiga.

3.4 Analys av data

Analys av kvantitativa data har idag programvaror som hjälpmedel för de statistiska analyserna. Programvarorna har underlättat för forskaren att analysera data, dock är det viktigt att ha i åtanke vilken data som analyseras och hur. Vissa statistiska analyser kan påvisa samband som egentligen inte finns eller är irrelevanta för forskningen om fel data matas in (Denscombe, 2000). Vidare menar författaren att så länge forskaren är medveten om för- och nackdelar, samt de begränsningar i slutsatserna som kan dras, kräver bra kvantitativ forskning inte avancerad statistisk analys.

För att kunna analysera data krävs vissa förberedelser. Den insamlade data måste kodas med siffror eftersom det är det enda formatet som lämpar sig för kvantitativ analys. Forskaren som redan vid utformningen av formuläret vet hur data skall kodas kan tidigt börja med kodningen och kategoriseringen och därmed bygga in dem i forskningsdesignen (Denscombe, 2000). Ett annat sätt att organisera i data är att göra frekvenssammanfattning vilket ger en tydligare bild av de vanligaste frekvenserna. Vid många frekvenser kan forskaren gruppera frekvensfördelningen för att göra det ännu lättare att läsa data (Denscombe, 2000).

Redan i utformningsstadiet av enkäten valde att använda oss av Likertskala samt andra rangordningsskalor där varje svarsalternativ tilldelades en siffra för den specifika frågan och därmed kodades svaren redan i insamlingen av data. Det gjorde att vi senare kunde effektivisera vårt arbete genom att föra över data direkt till SPSS utan att behöva koda data i efterhand.

Kodningen av data var inte helt genomförd när svaren hade kommit in, utan det fanns fortfarande frågor som inte hade blivit organiserade. Den berörda frågan var främst vilken ålder respondenten hade. För åldern valde vi att göra en grupperad frekvensfördelning då vi ville ha en tydlig data som var enkel att läsa. Dessutom kunde vi tack vare detta jämföra olika grupperade frekvenser med varandra i särskilda frågor och ställa oss frågan ”Varför ser det ut så här i olika ålderskategorier”.

När kodningen var klar sammanställde vi den insamlade data vi hade fått och presenterade det under resultat. För att få en mer överskådlig bild av resultatet utformade vi grafer och diagram utifrån den data som insamlats. Detta utgjorde också en ovärderlig hjälp vid analysarbetet eftersom vi tydligare kunde ana samband mellan olika frågor.

Det finns olika typer av kvantitativa data där bland annat data på nominalskalenivå samt på ordinalskalenivå är representerade. Data på nominalskalenivå är data som man räknar ihop och placerar i en viss kategori. Det kan innefatta kön, ursprung etc. På nominalskalenivå finns det inga större utrymmen för manipulation i statisktisk mening och nivån är den lägsta mätnivån för kvantitativa data. Det finns inte heller någon rangordning på kategorierna i nominalskalenivån, eller någon ordningsföljd för namnen (Denscombe, 2000).

Ordinalskalenivån innebär också en inräkning och kategorisering av data, men till skillnad från nominalskalenivån är kategorierna här rangordnade (Denscombe, 2000). Ordinalskaledata återses tydligast i frågeformulär där Likertskala används och innebär att data i varje kategori kan jämföras med data i andra kategorier.

Som nämnt tidigare har vi använt oss av Likertskalor samt andra rangordnade skalor i vår webbenkät. Vi har också använt oss av frågor där svaren inte kan rangordnas, som kön och vilka nätverk som används. Detta medför att vi i vår studie har data på både nominalskalenivå och ordinalskalenivå som skall analyseras i statistiska test.

När ett korrelationstest genomförs testar man sambandet mellan olika variabler. Ett korrelationstest är ett mått på styrkan av det linjära sambandet mellan variablerna och ger ett värde på 1 till -1. Ju närmare 1 desto starkare samband existerar (Wahlgren, 2005). Chi-två test testar också samband mellan variabler men till skillnad från korrelationstest behövs då minst 5 svar i varje ruta av tabellen. 20% av rutorna kan innehålla ett lägre värde men inget värde får understiga 1.

Då vi har något få respondenter för att genomföra chi-två tester valde vi att göra korrelationstester, där vi dessutom lättare kunde utläsa hur starkt respektive svagt sambandet mellan variablerna var. Eftersom vi använder oss av korrelationstest behöver vi dessutom inte kategorisera våra Likert-skalor för att få tillräckligt med svar i varje ruta, vilket hade varit fallet om vi hade använt oss av chi-två test.

3.5 Forskningens reliabilitet och validitet

Tillförlitligheten (reliabiliteten) är ett mått på hur väl förankrade forskningsresultaten är till valet av tillvägagångssätt vid undersökningen samt vilka data som har samlats in. Neutraliteten i materialet skall vara av sådan art att en annan forskare skall kunna få fram samma resultat om denne utförde undersökningen igen med samma respondenter. Denscombe (2000) menar att det kan vara svårt att mäta dessa mål men att forskaren kan ge undersökningen en större tillförlitlighet genom att dokumentera alla beslut som tagits genom arbetet. Alla val och metoder skall utförligt skrivas ned så att läsaren enkelt kan följa hela arbetet från inledning till slutsats.

Reliabiliteten (tillförlitligheten) och validiteten (riktigheten) är viktiga delar i alla typer av forskning. Det är viktigt för tillförlitligheten att forskaren verkligen undersöker det som var tänkt att undersökas (Patel och Davidsson, 1995).

Operationaliseringen av våra undersökningsområden var ett viktig steg för att höja validiteten i vårt arbete. Vi delade upp begreppen integritet och säkerhet i flera undergrupper för att på så sätt säkra att vi inte skulle missa relevanta frågor. Innan webbenkäten gick ut live på nätverken genomförde vi pilottester på frågorna med resultatet att vi fick göra ett fåtal språkliga ändringar där formuleringarna inte var korrekta eller frågorna var otydliga. Kvale (1997) menar att pilottester borgar för en god validitet vid datainsamling. Tillförlitligheten stärktes också genom pilottesterna genom att kontrollera att vi definierat begreppen ordentligt. En ordentlig genomgång på frågorna efterföljde piloten för att säkerställa att orden i frågorna inte skulle kunna betyda en sak för en respondent men något annat för nästa respondent.

Pilottestet gav oss dessutom möjlighet att tillfråga respondenterna hur de uppfattade enkäten, så att deras svar överensstämde med vad vi menade att undersöka.

Faktumet att det var en webbenkät gjorde att vi inte kan ställa vidare frågor till respondenterna, detta försökte vi kompensera med att även ha med öppna frågor där respondenten kunde skriva fritt.

Ett sätt att ytterligare förstärka validiteten på studiens resultat hade varit att följa upp genom observationer där användare hade fått applicera rekommendationerna på sitt agerande i sociala nätverk.

3.6 Metodkritik

Vår uppfattning om metoden som vi använde vid insamling av data är att den fungerat bra i huvudsak. Den kvantitativa ansatsen och val av enkätundersökning passade väl in i det område vi ville undersöka och webbenkäten underlättade och snabbade upp arbetet med kodning och analys avsevärt.

Operationaliseringen som gjordes när enkätfrågorna utformades mynnade ut i fler frågor som respondenterna fick svara på. Vi anser dock att vi hade kunnat ge operationaliseringen och frågeformuleringarna lite mer tid för att fånga upp ytterligare följdfrågor i form av öppna frågor. Detta hade kunnat stärka några av de förväntningar vi hade på resultatet på några frågor och underlättat arbetet med analysen. Vi har också ett fall av att vi har gett en fråga fel svarsalternativ vilket ledde till att det blev svårare att analysera den och jämföra den med en liknande fråga. Resultatet av jämförandet hade kunnat vara intressant för att se hur användarna förhöll sig till två liknande frågor.

Vi anser att vi hade velat ha in fler enkätsvar än de 77 giltiga svar vi fick in. Detta hade varit möjligt om vi hade fått färdigt enkäten lite tidigare och haft den online en vecka till. Därigenom kunde vi ha skickat ut en till påminnelse samt publicera den på fler lämpliga informationskanaler. Fler respondenter hade kunnat leda till att vi hade sett starkare samband mellan olika variabler och därigenom få en starkare reliabilitet.

Som vi beskrev i avsnittet om valet av metodansats så utförde vi endast studier på användares beteende genom enkäten. Vi hade också kunnat utföra en workshop med användare för att faktiskt observera beteendet men inom tidsramen fanns inte denna möjlighet tillgänglig för att få ett resultat som speglade den kvantitet som vi fick in via enkäten.

4 Resultat

4.1 Resultat kartläggning av sociala nätverk

Här diskuteras de tre nätverk som har studerats. Kartläggningen har gjorts genom att studera de data som är nödvändiga all delge vid skapande av profil samt vilka inställningar som finns tillgängliga för användaren.

4.1.1 Match.com

Match.com är en webbsida som fokuserar på att användarna söker efter en livskamrat med hjälp av en profil där användaren presenterar sig själv och fyller i information om dennes intressen. Genom att fylla i intressen och annan information kan systemet sedan matcha fram eventuella partners som kan vara lämpliga kandidater. Ju mer användaren delger om sig själv desto närmare matchning kan systemet göra. Detta medför att det kan vara lockande för användaren att fylla ut med så mycket information som möjligt om sig själv. Det finns dock en del inställningar som kan göras för att bli mer anonym som att stänga av visningen av riktigt namn och adress.

Det finns dock inget enkelt sätt att radera sin profil på nätverket. Det går däremot att inaktivera så att den inte längre visas publikt eller hamnar som resultat i en sökning.

Det som är framträdande vid skapande av en profil på Match.com är att det är mycket information som skall fyllas i för att göra den sökbar. Det som kan göra detta nätverk till ett eventuellt hot mot användarens integritet är att själva syftet med det är att ge användaren förslag på potentiella partners och matchningen fungerar bättre ju mer information som användaren delar med sig. Användarvillkoren som måste godkännas vid skapandet av en profil på Match.com är indelat i ett avsnitt om personlig integritet och ett avsnitt med användningsvillkor. Avsnittet om personlig integritet tar bland annat upp vad nätverket måste samla in om användaren för att kunna fungera ordentligt och vad denna information används till samt vem som har tillgång till den. De allmäna användningsvillkoren är ett lite större dokument som är indelat i 12 stycken som behandlar användarens och nätverkets rättigheter och skyldigheter. En innehållsförteckning gör det lätt att söka i dokumentet efter det som är intressant.

4.1.2 Facebook

Facebook har sedan sin start 2004 vuxit till ett stort socialt nätverk med över 400 miljoner medlemmar. På sidan kan användaren göra allt ifrån att hålla kontakt med sina vänner till att spela spel och skapa demonstrationer.

Vid skapandet av profil krävs det att användaren uppger sitt fulla namn, email-adress, kön och födelsedatum då Facebook har en åldersgräns på 13 år. Användningsavtalet är ett paragrafindelat dokument där de 18 paragraferna refererar till varandra vilket gör att det blir ett rörigt dokument att läsa. Villkoren behandlar bland annat vad användaren och nätverket har för rättigheter och skyldigheter samt vem det är som äger det material som läggs upp på webbsidan. Det som skiljer

Facebook från de andra två nätverk som kartlagts är att det på nätverket finns möjlighet för tredje part att tillverka applikationer där programmeraren själv ansvarar för det som skapas och läggs upp. Detta gör att Facebook inte tar något ansvar om en användare skulle råka illa ut pga användandet av tredjepartsapplikation.

Användaren kan delge mycket information om sig själv om han/hon vill men det är inte nödvändigt att fylla i alla fält på profilen. Det finns också möjlighet att fylla i all information och sedan välja vilka som har tillgång att se den. Inställningsmöjligheterna på facebook är många och förklaringarna till vad de gör är inte alltid självklara. Under kartläggningen kom det fram att alla inställningar inte fungerade som de skulle och information som skulle ha varit dold för en viss grupp användare inte har varit det. Detta medför att en stor försiktighet bör iakttas om du vill lägga upp information som inte är ämnad för allmänheten. Facebook själva varnar för detta i användarvillkoren där de säger att tjänsten levereras som den är och att användaren själv ansvarar för det material som laddas upp till sidan.

4.1.3 Twitter

Twitter är ett nätverk där användaren skriver statusmeddelanden, ”twittrar”. Det kan liknas vid en dagbok där du håller dina vänner uppdaterade om vad du gör för tillfället. Nätverket tillåter användaren att lägga till bilder, videos, länkar och att lägga till en plats han/hon ”twittrar” ifrån. Denna plats kan t.ex. vara hemma eller på jobbet. Det går snabbt att komma igång med Twitter; det enda som behövs för att skapa ditt konto är ditt fulla namn, din email-adress och ett lösenord och sedan är du redo att skapa dina egna statusmeddelanden. Funktioner för att hitta dina vänner som twittrar genom att söka efter email eller på namn finns vilket gör dem enkla att hitta. Detta gör att nätverket är öppet och det är lätt att hitta personer vars status du är intresserad av. Även Twitter har ett användningsavtal som är tvådelat. Det ena handlar informationsinhämtning. Där står beskrivet vilken information som inhämtas från användaren, vem som har tillgång till den och vad den får användas till. Användarvillkoren på Twitter är kortare än de andra två. Det har en utformning som gör att det är lätt att ta till sig med då det är bra uppdelat och inte alltför långt. Även här tas användarens och nätverkets rättigheter och skyldigheter upp

Om användaren inte vill att sina uppdateringar skall kunna ses av vem som helst kan man ställa in att alla som vill följa dem måste godkännas först. Detta medför att du kan välja exakt vilka som kan följa dig. Denna funktion är dock avstängd som standard.

Twitter är ett användarvänligt utformat nätverk där det är lätt att förstå vad de olika funktionerna gör och inställningarna är så pass få att det är överskådligt.

Vi skapade en tabell (se tabell 4.1) för att plocka fram det som var framträdande hos respektive nätverk.

	Match.com	Facebook	Twitter
Obligatorisk info som anges vid registrering av användarkonto	Acceptera användarvillkor	Acceptera användarvillkor	Acceptera användarvillkor
	Vilken typ av relation som söks	Fullständigt namn	Fullständigt namn
	Vilket åldersspann du tillhör	Email-adress	Email-adress
	Födelsedatum	Lösenord	Lösenord
	Postnummer	Kön	
	Email-adress	Födelsedag	
	Lösenord		
Tillgängliga inställningar för ökad säkerhet	Du kan stänga av visningen av ditt fulla namn och din adress.	Det finns möjlighet att kontrollera vilka som har tillgång att se det material som du laddat upp.	Lägga till en plats du ”twittrar” ifrån. T.ex. Hemma eller jobbet. Är avstängd som standard
	Det går inte på ett enkelt sätt att radera sin profil. Däremot går det att inaktivera den så att den inte är synlig längre.	Du kan kontrollera vilka som har tillgång till din kontaktinformation och vilka som kan lägga till dig som vän.	Skydda inlägg. Detta innebär att du måste godkänna alla personer som vill följa dina inlägg. Avstängt som standard.
		Du kan kontrollera vilken av din information dina vänner kan dela med sig av.	Du kan välja att få email när en person vill följa dina inlägg.
Slutkommentar	Hela poängen med sidan är att andra personer skall kunna hitta just dig. Profilinformationen byggs till stor del upp av fritextrutor där du själv tar ansvar för det du delar med dig av.	Facebook är ett stort nätverk med många inställningar och osynliga informationsutbyten. Vi upplever också att inställningarna som görs inte alltid sparas. Många av formuleringarna på de inställningar som kan göras är otydliga.	Twitter är ett mycket användarvänligt nätverk. Tydliga formuleringar angående vad de olika inställningarna gör. Få inställningar gör det också mer överskådligt.

Tabell 4.1 Kartläggning

4.2 Presentation av studiens resultat

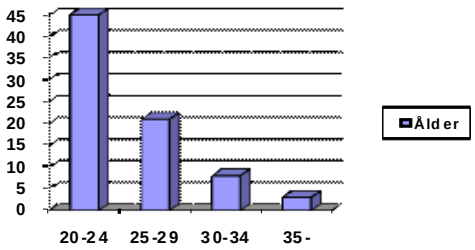
Under den vecka som webbenkäten fanns tillgänglig skickades den ut till 170 personer på två nätverk samt fanns tillgänglig som länk på det tredje nätverket. Av dessa (minst) 170 respondenter inkom 92 svar. Av dessa svar var 15 stycken ogiltiga och fick raderas från studien då de inte var komplett ifyllda. Det gav en svarsfrekvens på ca 45% efter att de ogiltiga svaren raderats.

I presentationen av resultatet har vi valt att genomgående addera svarsalternativ 1 och 2 till ”instämmer inte” samt 4 och 5 till ”instämmer” för att ge ett mer överskådligt resultat. De figurer och tabeller som finns redovisar samtliga svarsalternativ.

4.2.1 Bakgrundsfrågor

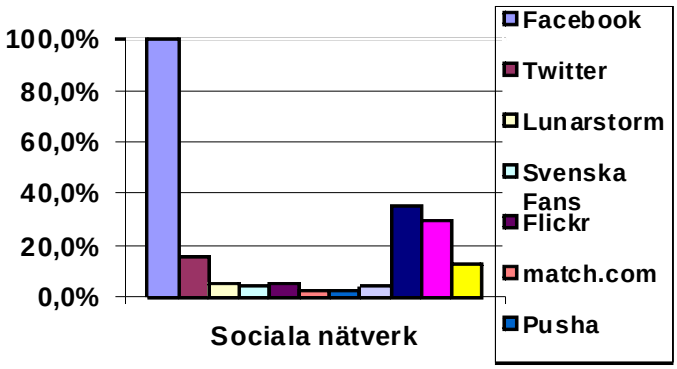
I detta avsnitt behandlas frågorna 1-4 som rör den bakgrund respondenten har och som senare kommer att ligga till grund för test av vissa statistiska samband.

Fördelningen av kvinnor och män i studien visade sig vara relativt jämnt fördelat, av de 77 respondenterna var 41 st kvinnor och 36 st män. Medelåldern hos respondenterna var 25 år. För att tydligare kunna utläsa skillnader i åldersgrupper valde vi att kategorisera ålder i resultatet. I kategorin 20-24 år fanns det 45 respondenter; i kategorin 25-29 år 21 respondenter; 8 respondenter i kategorin 30-34 år samt 3 respondenter som var 35 år eller äldre. Fördelningen av de olika åldersgrupperna illustreras i figur 4.1.



Figur 4.1 Åldersfördelning

Fråga 3 och 4 rörde vilka sociala nätverk som respondenten använder sig av idag. Respondenten hade 10 olika nätverk att välja mellan, samt att man kunde fylla i annat nätverk om ens nätverk inte fanns representerat. Det visade sig att alla respondenter hade ett Facebook-konto. Andra nätverk som hade flertalet användare var Windows Live (35,1%), egen blogg (29,9%), Twitter (15,6%) samt alternativet annat nätverk (13%). Vilka nätverk som användes av respondenterna kan ses i Figur 4.2. Bland de övriga nätverk som respondenterna använde nämndes; LinkedIn, Qx, Sylvia, porrigt.se, Google Wave, e-kontakt, Helgon samt forum för specialintressen.



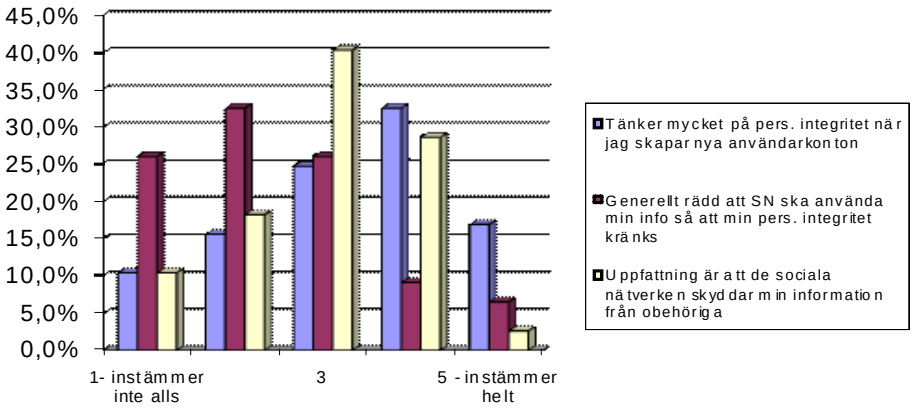
Figur 4.2. Användare på sociala nätverk i procent

4.2.2 Integritetsfrågor

Detta avsnitt presenterar resultatet av de frågor som rör integritet och integritetshot på sociala nätverk, vilka är utformade under operationaliseringen av begreppen.

Figur 4.3 Integritetsfrågor

Frågorna 5, 8 och 9 undersökte huruvida användarna tänker på sin personliga integritet när de skapar användarkonton samt om de är oroliga över huruvida de sociala nätverken skyddar deras information eller använder den på ett eventuellt kränkande sätt. Resultatet är sammanställt i figur 4.4.

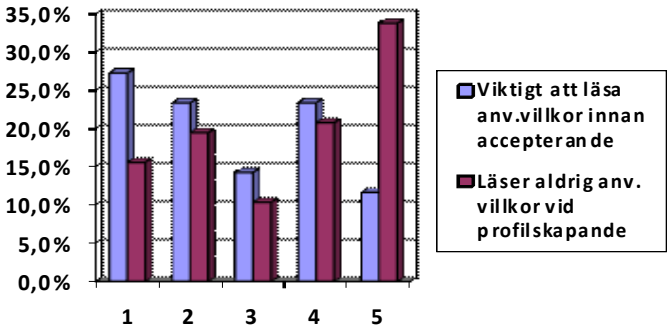


Figur 4.4 Inställning till integritet

Resultatet för dessa frågor går i viss mån isär. 49,4% uppger att de tänker mycket på sin personliga integritet när de skapar nya användarkonton, 26% instämmer inte i påståendet. På frågan ”*Generellt sätt är jag rädd att de sociala nätverken ska använda min information på ett sätt som gör att min personliga integritet kränks*” instämde 14,6% medan 58,5% av respondenterna inte instämmer i påståendet. 31,2% har dessutom uppfattningen att de sociala nätverken skyddar deras information från obehöriga, en uppfattning som 28,6% av respondenterna inte delar. 40,3% av respondenterna lägger sig på en neutral nivå i frågan.

I enkäten ställdes det också frågor angående användarvillkor och huruvida användaren läser dem före de accepterar eller ej. Resultatet blev att majoriteten av respondenterna anser att det inte är viktigt att läsa användarvillkoren innan de accepterar dem, över 50 % har svarat alternativ 1 eller 2 (1=instämmer inte alls). Detta bekräftas av de 54,6 % som har svarat 4 eller 5 (5=instämmer helt) på frågan angående att de aldrig läser användarvillkor vid profilskapande. Trots den höga procenten gällande de som inte anser det vara viktigt att läsa användarvillkor och inte gör det, så finns det också en relativt hög andel som anser det vara viktigt att läsa användarvillkoren. Av respondenterna var det strax över 35 % som ansåg att det är viktigt att läsa användarvillkoren och

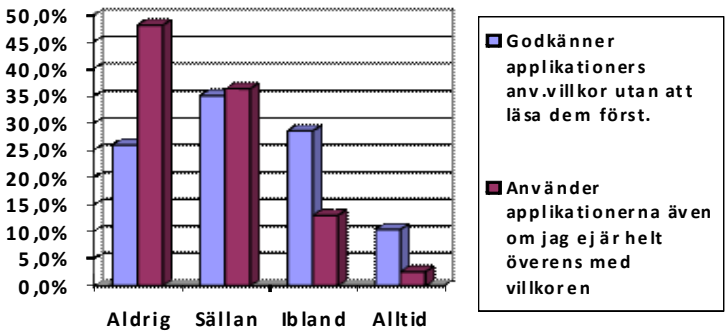
precis lika många inte instämde i frågan ”*läser aldrig användarvillkoren före profilskapande*”. Fördelningen kan ses i figur 4.5.



Figur 4.5 Användarvillkor

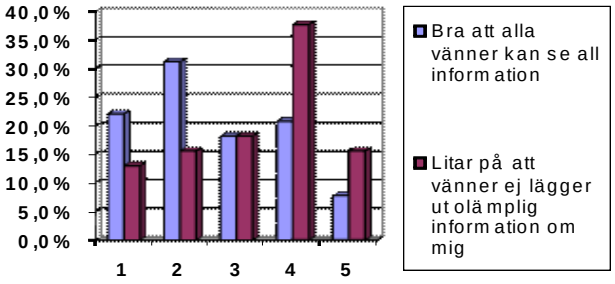
För att bekräfta de uppgifter som respondenterna svarade på i början av enkäten gällande användarvillkor ställdes det några frågor till i ämnet. På frågan ”*Jag godkänner de sociala nätverkens användarvillkor utan att läsa dem först*” svarade 68,8% ja och 31,2% nej. Det är några procentenheter mindre än vad respondenterna tidigare svarat angående frågan ”*Läser aldrig användarvillkoren när jag skapar ny profil*”.

Enkäten tog även upp hur användarna ställde sig till villkorsfrågan fast angående applikationer. Frågorna ”Jag *godkänner applikationers användarvillkor utan att läsa dem först*” samt ”*Jag använder applikation även om jag inte är helt överens med användarvillkoren*” ställdes till respondenterna. Även här uppgav flertalet respondenter att de inte läser användarvillkoren för applikationer innan de godkänner dem, 26 % svarade ”aldrig” och 35,1% svarade ”sällan”. Något förvånande var resultatet att det endast är strax under hälften, 48,1%, som aldrig skulle använda applikationerna om de inte är helt överens med användarvillkoren. Respondenternas svar ses i figur 4.6.



Figur 4.6 Användarvillkor och applikationer

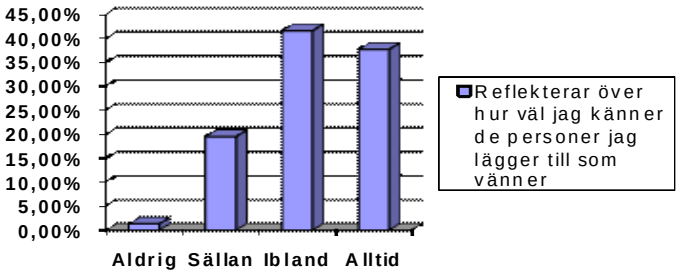
Respondenterna fick svara på ett antal frågor gällande vilka man lägger till som vänner och informationen som vännerna har tillgång till. 28,6% av respondenterna (de som svarat 4 & 5) anser att det är bra att alla vänner kan se all information om dem själva, medan 53,3% (de som svarat 1 & 2) inte tycker att det är bra att alla vänner har tillgång till hela ens personliga information. Majoriteten av respondenterna litar på sina vänner; 53,3% uppger att de inte tror att deras vänner lägger upp olämplig information om dem medan 28,6% menar att de inte litar på att ingen olämplig information läggs upp. Hur respondenterna svarade visas i figur 4.7.



Figur 4.7 Vänner-information

Av de 77 svar vi har fått in svarade 20 st att de endast lägger till personer de känner som vänner, medan 57 st lägger till även obekanta som vänner (26% respektive 74%). Samtidigt anser 50,6% att det är mycket viktigt att fundera över vilka som läggs till som vänner, 18,2% anser att det är viktigt och 31,2% anser att det inte är fullt så viktigt eller inte alls viktigt.

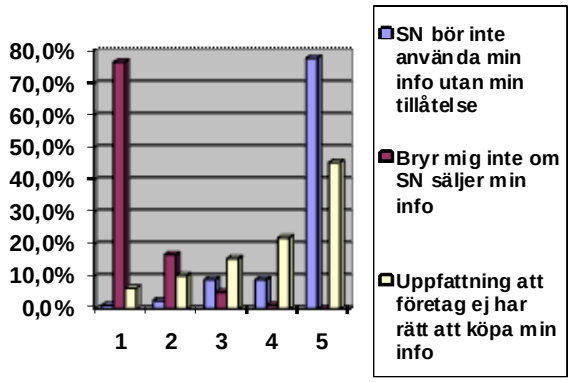
Våra respondenter uppger också att 37,7% av dem alltid reflekterar över ifall de känner personen de lägger till som vän, bara 1,3% reflekterar aldrig över vilken relation man har till vännen. 61,1% säger att de sällan eller ibland reflekterar över hur väl de känner personen som ska läggas till som vän (se figur 4.8).



Figur 4.8 Reflektion över vänner

I enkäten ställdes frågor som rörde huruvida de sociala nätverken har rätt att använda och sälja användarens personliga information eller ej. Totalt ansåg 87% av respondenterna att nätverken

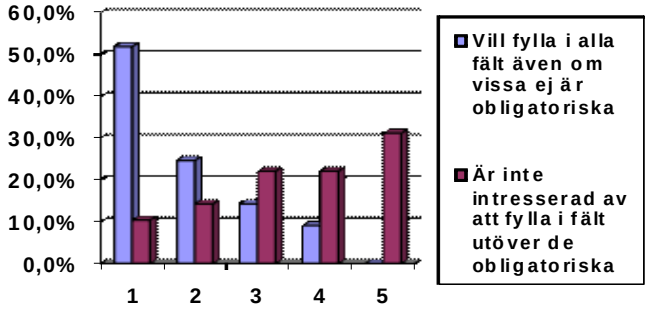
inte har rätt att använda den personliga informationen utan användarens tillåtelse. Endast 3,9% instämde inte i påståendet ”*Min uppfattning är att de sociala nätverken inte bör använda min information utan min tillåtelse*”. Följdfrågan ”*Jag bryr mig inte om huruvida de sociala nätverken säljer information om mig till andra företag*” fick majoriteten av respondenterna att tycka tvärtom, hela 93,5% instämde inte i påståendet och det var ingen som instämde helt. Den sista frågan som rörde den personliga informationen och de sociala nätverkens rätt att sälja informationen eller ej, löd ”*Min uppfattning är att andra företag inte har rätt att köpa min information från de sociala nätverken*”. Även här var en klar majoritet, 67,6%, överens med påståendet i frågan, 16,9% instämde inte. Fördelningen av svar i frågorna visas i figur 4.9.



Figur 4.9 Sociala nätverkens rätt att använda personlig information

Nästa del av enkäten rörde profilskapande, där den första frågan var ”*Jag lämnar alltid ut mitt rätta namn vid profilskapande*”. Av de 77 respondenterna svarade 59,7% ”ja” och 40,3% ”nej”.

Vi frågade också om vilka fält vid profilskapandet som respondenten var villig att fylla i, om de endast ville fylla i de obligatoriska fälten eller om även de icke-obligatoriska fälten var intressanta att fylla i. 53,3% svarade att de inte är intresserade av att fylla i fält utöver de obligatoriska, medan 24,3% inte instämde i samma fråga. När vi vände på frågan och sa ”*Jag vill fylla i alla fält även om vissa inte är obligatoriska*” svarade 76,6% att de inte instämde i påståendet. Endast 9,1% instämde, och då instämde ingen respondent helt. Utfallet visas i figur 4.10.



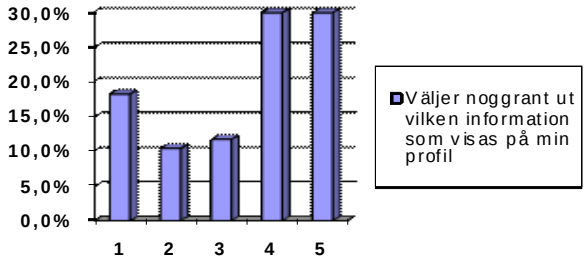
Figur 4.10 Att vilja lämna ut information – obligatoriskt eller ej

Mot slutet av integritetskapitlet i enkäten ställdes frågor angående mängden information som visas i profilen samt hur användaren påverkar vilken information som visas. Den första frågan gällde huruvida användaren tyckte att det var viktigt att kunna påverka mängden information som visas på det sociala nätverket. 97,4%, dvs 75 av de 77 respondenterna ansåg att det är viktigt att kunna påverka vilken information som visas, endast 2 stycken tyckte inte att det var viktigt. Vi ställde också frågan ”*Jag har mycket information om mig på min profil*” där 29,9% svarade ”ja” och 70,1% svarade ”nej”. Resultatet ses i tabell 4.2.

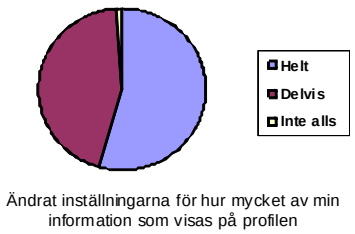
	Ja		*Nej*	
Jag tycker det är viktigt att kunna påverka hur mycket information som visas om mig på det sociala nätverket.	75	97,4%	2	2,6%
Jag har mycket information om mig på min profil.	23	29,9%	54	70,1%

Tabell 4.2 Informationsmängd och påverkan

Frågor angående ifall respondenten hade ändrat inställningarna för hur mycket av den personliga information som visas ställdes, liksom ifall respondenten noggrant väljer ut vilken information som visas. 59,8% angav att de noggrant väljer ut vilken information som visas medan 28,6% säger att de inte väljer ut informationen noggrant. Samtidigt menar 98,7% att de har delvis eller helt har ändrat inställningarna för vilken information som visas på nätverket, bara 1,3% har inte ändrat något alls. Resultatet illustreras i figur 4.11a och 4.11b.



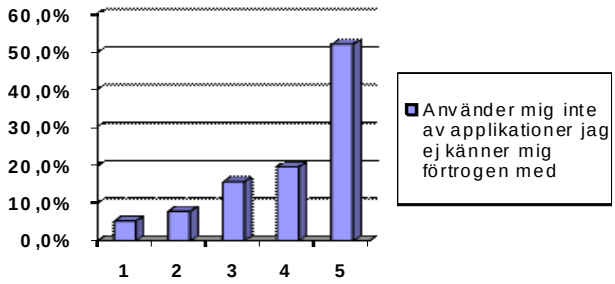
Figur 4.11a Informationsvisning



Figur 4.11b Ändring av informationsvisning

De sista frågorna i enkäten under avsnittet Integritet berörde applikationer. Vi ställde först frågan ”*Jag använder mig av applikationer*” för att sedan följa upp med frågan ”*Jag använder mig inte av applikationer som jag inte känner mig förtrogen med*”. 50,6% av respondenterna uppgav att de använder sig av applikationer medan resterande 49,4% inte gör det. Majoriteten av respondenterna, 71,4%, uppger att de inte använder sig av applikationer de inte känner sig

förtrogna med, medan 13% menar att de använder applikationer trots att de inte känner sig förtrogna med dem. Hur respondenterna svarat i den senare frågan kan ses i figur 4.12.



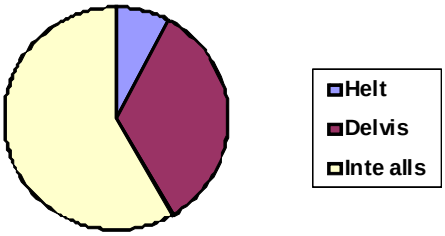
Figur 4.12 Förtrogenhet med applikationer

4.2.3 Säkerhetsfrågor

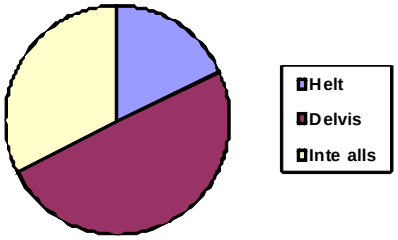
I det här avsnittet presenteras resultaten från de frågor i enkäten som rör säkerhet och säkerhetshot.

Figur 4.13 Säkerhetsfrågor

Det första området som berördes i säkerhetsavsnittet var lösenord och lösenordsvanor. Vi undersökte huruvida lösenorden som respondenterna använder sig av är slumpmässigt utvalda eller har en koppling till deras personliga liv. Resultat blev att 7,8% av respondenterna har lösenord som helt är kopplat till deras personliga liv och 18,2% har helt slumpmässigt utvalda lösenord. Vi fick också svaren att 49,4% har lösenord som delvis är slumpmässigt utvalda och 33,8% har lösenord som delvis har koppling till respondentens personliga liv. Respondenternas svar finns återgivna i figurerna 4.14a och 4.14b.



Figur 4.14a Personligt lösenordsval



Figur 4.14b Slumpmässigt lösenordsval

Vi ville också undersöka medvetenheten hos användarna om riskerna med att använda samma lösenord på flera olika konton och ställde därför frågorna ”*Jag är medveten om att samma lösenord på flera konton ökar säkerhetsrisken*” samt ”*Jag använder mig av flera olika lösenord*”. Större delen av respondenterna svarade ”ja” på båda frågorna, 92,2% respektive 87%. Resultatet presenteras i tabell 4.3 nedan.

	Ja		Nej	
Jag är medveten om att samma lösenord på flera konton ökar säkerhetsrisken	71	92,2%	6	7,8%
Jag använder mig av flera olika lösenord	67	87%	10	13%

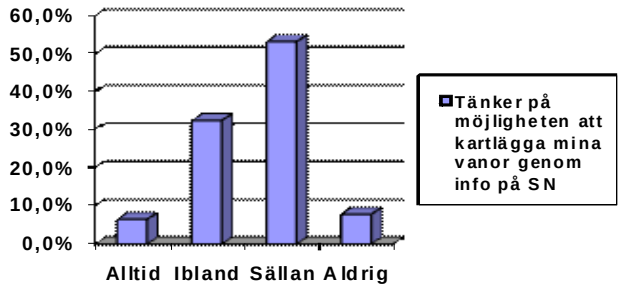
Tabell 4.3 Medvetenhet om säkerhetsrisker för lösenord

För att få en uppfattning om hur mycket information respondenterna kan tänka sig att lämna ut till en person de inte känner närmare ställde vi frågan ”*Jag ger ut information om mig själv till en kollega som efterfrågar det*”. Denna fråga ställdes för att undersöka medvetenheten om social engineering och ett möjligt scenario, så som att lämna ut information till en kollega som efterfrågar det . Vi ställde därefter följdfrågan *”Om nej, vilken information kan du inte tänka dig att lämna ut?*”. 68,8% angav att de kunde tänka sig att ge ut personlig information till en kollega. Bland de 31,2% som svarade ”nej” på frågan angavs bland annat följande anledningar:

- Ekonomi
- Sjukdomar
- Familjeangelägenheter
- Personnummer
- Kreditkortsnummer
- Bilder från fester
- Lösenord
- Inloggningsuppgifter till sociala nätverk
- Det som ej är relaterat till arbetet

Vi ställde även frågan ”*Jag berättar inget om mig själv om jag inte känner personen jag talar med*” där 36,4% instämde helt, 28,6% instämde inte och 35,1% lade sig i mitten och varken instämde eller ej.

I enkäten fanns även ett avsnitt som behandlade medvetenhet om kartläggning av vanor och andra kriminella attacker på sociala nätverk. Vi undrade ifall respondenterna tänkte på att möjligheten att kartlägga deras vanor genom information på sociala nätverk finns. 6,5% svarade att de alltid tänker på att möjligheten finns, 32,5% tänkte på det ibland, 53,2% sällan och 7,8% aldrig. För tydligare överblick, se figur 4.15.

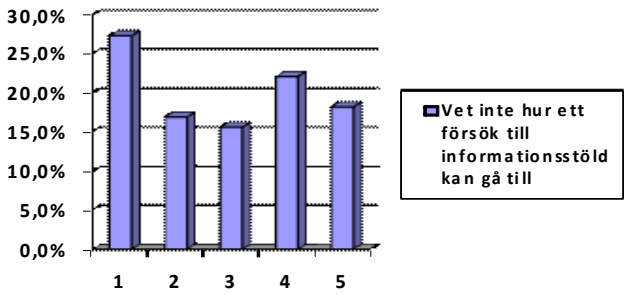


Figur 4.15 Medvetenhet om kartläggningsrisk

Vi ställde även frågan om respondenterna var medvetna om att de kan utsättas för kriminella attacker på de sociala nätverken, där 63,6% svarade att de är medvetna om risken och 36,4% inte är medvetna om att risken finns. Som följdfråga fick de som svarat ”ja” lista attacker de kände till. Följande kom fram i undersökningen:

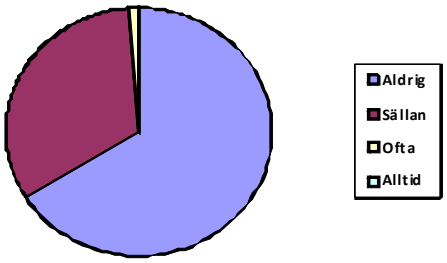
- Hackers
- Identitetsstöld
- Kontokortsstöld
- Kränkning
- Hets mot folkgrupp
- Social engineering
- Bedrägeri
- Phishing
- Spam-mail
- Utpressning
- Mobbing
- Inbrott i hem efter kartläggning

Enkäten fortsatte med att fråga om respondenten vet hur ett försök till informationsstöld kan gå till och ifall respondenten är medveten om att informationsstöld kan utföras genom social kommunikation. 44,2% av respondenterna uppger att de vet hur ett försök till informationsstöld kan gå till och nästan lika många, 40,3%, uppger att de inte vet hur ett försök kan gå till (se figur 4.16). Däremot uppger 80,5% att det var medvetna om att informationsstölder kan ske via social kommunikation, 19,5% var inte medvetna om det.



Figur 4.16 Medvetenhet om hur ett försök till informationsstöld kan gå till

En annan fråga som ställdes till respondenterna var huruvida de öppnar den skräppost som kommer till deras mail. Respondenterna svarade till 66,2% att de aldrig öppnar skräppost, 32,5% svarade sällan, 1,3% svarade ofta och det var ingen av respondenterna som uppgav att de alltid öppnar skräpposten som kommer på mailen. Resultatet ses i figur 4.17.



Figur 4.17 Öppnar skräpposten som kommer till mailen

De sista frågorna i enkäten behandlade medvetenhet om applikationers tillgång till personlig information. Den första frågan var ”*Jag är medveten om att de applikationer jag använder får tillgång till min personliga information*” och den andra var ”*Jag är medveten om att applikationer kan få tillgång till min personliga information genom att mina vänner har godkänt villkoren*”. Det visade sig att 81,8% av respondenterna var medvetna om att applikationer de själva använder får tillgång till deras personliga information men att bara 40,3% visste att applikationerna kan få tillgång till deras personliga information genom att vänner använder dem. Se tabell 4.4.

	Ja		*Nej*	
Jag är medveten om att de applikationer jag använder får tillgång till min personliga information	63	81,8%	14	18,2%
Jag är medveten om att applikationer kan få tillgång till min personliga information genom att mina vänner har godkänt villkoren	31	40,3%	46	59,7%

Tabell 4.4 Medvetenhet om applikationers tillgång till information

5 Analys och diskussion

Nedan följer diskussion och analys av det resultat som samlades in med hjälp av den empiriska studien. Till stöd användes vår teoretiska referensram.

Då vi sammanställde resultatet från vår studie visade det sig att åldersfördelningen bland respondenterna inte var särskilt varierande. Våra respondenter befann sig huvudsakligen i åldrarna 20 till 30 år. Det kan medföra att rekommendationerna som presenteras i slutsatsen inte är tillämpbara på alla ålderskategorier i de sociala nätverken.

5.1 Integritet

Integritetens kärna ligger hos användaren, vad som upplevs i begreppet kan skilja sig från person till person (Brodie *et al.*, 2005), vilket även *inställningen till den personliga integriteten* gör. Som ett första led ville vi därför undersöka hur våra respondenters syn på integritet är. Vi ville veta hur mycket de tänker på integriteten och hoten mot den när de skapar nya användarkonton. I förhållande till detta ville vi sedan se om det fanns något samband till att man generellt sätt är rädd över hur de sociala nätverken använder informationen. Flertalet av dem som inte tänker på sin integritet är inte heller rädda för att kränkas av de sociala nätverken. Vi kan dock konstatera att ca 58% inte är oroliga över kränkning pga. hur nätverken använder informationen. Korstabuleringen visade också att det var många som instämde i båda påståendena. Vi genomförde därför ett korrelationstest för att kunna se om det fanns samband mellan hur mycket man tänker på integriteten och hur rädd man är att den kränks (se tabell 5.1).

Crosstab

Count

		Fr8: Generellt rädd att SN använder min info på ett sätt som gör att integriteten kränks			
		Instämmer inte	Neutral	Instämmer	Total
Fr5: Tänker mycket på personlig integritet	Instämmer inte	15	3	2	20
	Neutral	13	6	0	19
	Instämmer	17	11	10	38
Total		45	20	12	77

Correlations

		Fråga 5:Tänker mycket på personlig integritet när skapar nya konto	Fråga 8: Generellt rädd att SN anv. info. --> pers.kränkning
Fråga 5:Tänker mycket på personlig integritet när skapar nya konto	Pearson Correlation	1	,355**
	Sig. (2-tailed)		,002
	N	77	77
Fråga 8: Generellt rätt att SN anv. info. --> pers.kränkning	Pearson Correlation	,355**	1
	Sig. (2-tailed)	,002	
	N	77	77

**. Correlation is significant at the 0.01 level (2-tailed).

Tabell 5.1 Personlig integritet

Vi kan konstatera att det finns ett samband enligt korrelationstestet mellan hur mycket man tänker på sin integritet och oron för hur ens information används, även om sambandet är ganska svagt. För att kunna jämföra hur respondenterna svarade gjorde vi även en korstabulering mellan ”*tänker mycket på min personliga integritet*” och ”*uppfattning att de sociala nätverken skyddar min information*”. Här kan vi dock se i korrelationstestet att det inte finns något samband (se tabell 5.2).

Crosstab

Count

		Fr9: Uppfattning att SN skyddar min info			
		Instämmer inte	Neutral	Instämmer	Total
Fr5: Tänker mycket på personlig integritet	Instämmer inte	5	10	5	20
	Neutral	6	7	6	19
	Instämmer	11	14	13	38
Total		22	31	24	77

Correlations

		Fråga 5:Tänker mycket på personlig integritet när skapar nya konto	Fråga 9: Uppfattning SN skyddar min info
Fråga 5:Tänker mycket på personlig integritet när skapar nya konto	Pearson Correlation	1	,077
	Sig. (2-tailed)		,504
	N	77	77
Fråga 9: Uppfattning SN skyddar min info	Pearson Correlation	,077	1
	Sig. (2-tailed)	,504	
	N	77	77

Tabell 5.2 Skydd av information från sociala nätverkens sida

Vår slutsats av detta är att det inte finns något samband mellan uppfattningen att nätverken skyddar informationen och att de tänker mycket på sin integritet. Här var svaren mer jämnt fördelade i korstabuleringen, vissa ansåg att nätverken skyddar informationen mer än andra. Det var också många som förhöll sig neutrala och inte ville ta ställning, oavsett vad man ansåg om den personliga integriteten. Vi menar också att utifrån korstabuleringarna kan vi konstatera att även om användarna inte är rädda för hur nätverken använder deras information så betyder det inte att de anser att nätverken skyddar deras information.

Att det är en stor skillnad i hur användarna svarar på de två påståendena gör att vi ställer oss undrande inför varför det skiljer sig. Vi tror att den stora andel som valde att svara neutralt i att nätverken skyddar deras information tyder på att användarna inte har någon mer ingående kunskap om hur de sociala nätverken använder informationen som samlas in. Skulle det förhålla sig på detta vis är det intressant att fundera över varför de inte är rädda att nätverken använder deras information på ett eventuellt kränkande sätt. Det skulle kunna bero på att de förseelser som har upptäckts snabbt har åtgärdats då media har hjälpt till att sprida dem och att nätverket därmed blir tvingade till att åtgärda felen. På så sätt är det möjligt att användaren känner sig trygg i vetskap om att förseelser rapporteras och åtgärdas snabbt. Dock är detta ingen garanti för att det förhåller sig så ifall en förseelse skulle drabba användaren själv. Vi menar att det är viktigt att tänka på sin integritet och hur nätverken använder informationen som lämnas ut.

Vid skapande av ett nytt konto hos ett socialt nätverk måste man som användare acceptera *användarvillkoren*. Vi upplever att dessa villkor ofta är alldeles för långa och komplicerade för att placera in dem i kontexten på webbplatserna, Flinn och Lumsden (2005) bekräftar detta i sin studie där användarna inte har några höga tankar att säga om villkoren. Språket som används är

dessutom ofta byråkratiskt och på de internationella sidorna återfinns de också endast på engelska vilket kan innebära svårigheter för personer som inte har så stor kunskap i språket.

Under kartläggningen av webbplatserna kunde vi konstatera att Facebook även hade sina användarvillkor tillgängliga på tyska, italienska, spanska och franska. Dock var det svårt att hitta i texten då punkterna refererar till varandra och läsaren får hoppa fram och tillbaka i texten som är 16 sidor lång. Dessutom ger Facebook tips på fler dokument som användaren bör läsa i slutet av villkoren. Detta har även Twitter vid sina användarvillkor om än i mindre utsträckning. Twitter har dessutom förslag på sidor ifall användaren har problem med överträdelser mot dessa villkor. Hos match.com är användarvillkoren på svenska och de har inga länkar som för användaren vidare. Däremot har även de två olika dokument; sekretesspolicy och allmänna villkor.

I vår studie ställde vi två frågor kring användarvillkor gällande profilskapande. Vi ville dels se hur användarnas inställning var, dels få reda på om de agerade efter sin inställning. Vi genomförde därför ett korrelationstest där vi ställde de två frågorna mot varandra, se tabell 5.3. Testet visar att det finns ett starkt samband mellan inställningen och agerandet. De som inte tycker att det är viktigt att läsa användarvillkoren innan man accepterar dem gör heller inte det. Vi kan i korstabuleringen konstatera att åtta (>10%) av våra respondenter tycker att det är viktigt att läsa användarvillkoren men agerar inte enligt sin inställning. Vi kan å andra sidan också se att det finns användare som inte tycker att det är viktigt att läsa användarvillkoren men ändå läser dem emellanåt.

Fr6: Viktigt att läsa anv.villkor innan accepterande * Fr7: Läser aldrig användarvillkor vid profilskapande Crosstabulation

Count

		Fr7: Läser aldrig användarvillkor vid profilskapande			
		Instämmer inte	Neutral	Instämmer	Total
Fr6: Viktigt att läsa anv.villkor innan accepterande	Instämmer inte	8	3	28	39
	Neutral	4	1	6	11
	Instämmer	15	4	8	27
Total		27	8	42	77

Correlations

		Fråga 6:Viktigt att läsa användarvillkor innan accepterar	Fråga 7: Läser aldrig anv.villkor när skapar ny profil
Fråga 6:Viktigt att läsa användarvillkor innan accepterar	Pearson Correlation	1	-,488**
	Sig. (2-tailed)		,000
	N	77	77
Fråga 7: Läser aldrig anv.villkor när skapar ny profil	Pearson Correlation	-,488**	1
	Sig. (2-tailed)	,000	
	N	77	77

**. Correlation is significant at the 0.01 level (2-tailed).

Tabell 5.3 Användarvillkor

Vi har i efterhand märkt att vi här saknar en följdfråga där respondenterna kunde beskriva varför de läser/inte läser användarvillkoren. Svaren från en sådan fråga hade kunnat vara intressant för att få en helhetsbild av sambandet och hade kunnat verifiera/dementera vår åsikt om att texterna är för långa och komplexa.

När vi konstruerade frågorna förväntade vi oss att en högre andel skulle instämma i båda frågorna, att de tycker det är viktigt men att de inte läser användarvillkoren. Att 39 respondenter, ca 50%, inte anser att det är viktigt att läsa användarvillkoren är oroande för den personliga integriteten då det är i användarvillkoren som denna fastställs. Det är däremot inte förvånande att 42 respondenter instämmer i att de inte läser användarvillkoren då dessa, som tidigare påpekat, ofta är långa och byråkratiska. Att en så stor andel inte läser användarvillkoren kan bero på att de, som Flinn och Lumsden (2005) noterar, tror att nätverken garanterar sekretessen och skyddar användaren när det finns villkor att acceptera.

Det vi konstaterar är att en hög andel av respondenterna inte anser det vara viktigt att läsa användarvillkoren vid profilskapande, då en stor mängd personlig information lämnas ut. Bristen på intresse för att läsa användarvillkoren kan leda till att de sociala nätverken har rätt att använda den personliga informationen hur de vill då användarna accepterar villkoren utan vidare betänkande.

På Facebook finns det också *applikationer* där användaren måste acceptera villkor för att kunna använda dem. Då vi hade ställt frågor angående användarvillkor när man skapar ny profil var det också intressant att ställa frågan om beteendet gällande villkor även är aktuellt för applikationer. Då vi ville se om det fanns ett samband mellan inställning och agerande också här genomförde vi därför ett korrelationstest där samma fråga som i föregående test ställdes i förhållande till

huruvida användarna godkänner applikationers användarvillkor utan att läsa dem först. Enligt testet är signifikansen tillräckligt stor för att kunna konstatera ett starkt negativt samband, se tabell 5.4.

Correlations

		Fråga 6:Viktigt att läsa användarvillkor innan accepterar	Fråga 24: Godkänner appars användarvillkor utan att läsa dem
Fråga 6:Viktigt att läsa användarvillkor innan accepterar	Pearson Correlation	1	-,407**
	Sig. (2-tailed)		,000
	N	77	77
Fråga 24: Godkänner appars användarvillkor utan att läsa dem	Pearson Correlation	-,407**	1
	Sig. (2-tailed)	,000	
	N	77	77

**. Correlation is significant at the 0.01 level (2-tailed).

Tabell 5.4 Applikationers användarvillkor

Vad vi kan se från dessa två test är att det skiljer sig mellan applikationers användarvillkor och de sociala nätverkens egna användarvillkor. Vi ville därför undersöka det tydligare genom att korstabulera de två (se tabell 5.5). Det som förvånar här är att siffran för de som instämmer i att de aldrig läser användarvillkoren för de sociala nätverken och som aldrig eller sällan godkänner applikationers användarvillkor utan att läsa dem först är hög.

Fr7: Läser aldrig användarvillkor vid profilskapande * Fr24: Godkänner applikationers användarvillkor utan att läsa dem först Crosstabulation

		Fr24: Godkänner applikationers användarvillkor utan att läsa dem först		
		Aldrig-Sällan	Ofta-Alltid	Total
Fr7: Läser aldrig användarvillkor vid profilskapande	Instämmer inte	20	7	27
	Neutral	7	1	8
	Instämmer	20	22	42
Total		47	30	77

Tabell 5.5 Korstabulering användarvillkor

Genom kartläggningen kan vi konstatera att applikationernas användarvillkor oftast är korta texter på några få meningar i kontrast till nätverkens användarvillkor. Applikationernas användarvillkor visas i samband med första gången applikationen ska användas och då den bara är ett fåtal meningar är den troligtvis lättare att ta till sig och orka läsa än vad nätverkets användarvillkor är. Vi kan ändå notera att även om det var flertalet som läser användarvillkoren till applikationer så är det också många som inte läser dem. Frågan om varför de inte läser dem uppkommer då dessa användarvillkor är särskilt lättillgängliga och lättförståeliga. Något som är än mer förvånande är att endast 48,1% av respondenterna aldrig skulle använda en applikation om de inte är överens med användarvillkoren. Andelen blev större när vi inkluderade de som svarat ”sällan” tillsammans med de som svarat ”aldrig”, andelen blev då 84,4%. Vi ansåg det vara intressant att ta reda på hur påståendet skulle stå sig i en korstabulering förhållande till påståendet att användarna inte använder sig av applikationer som de inte känner sig förtrogna med. Det visade sig att 65% inte använder sig av applikationer de inte har förtroende för samtidigt som de sällan eller aldrig använder applikationer där de inte är överens med villkoren (se tabell 5.6).

Fr28: Använder applikationer även om ej helt överens med användarvillkoren^Fr29: Använder mig inte av applikationer jag ej känner mig förtrogen med - Crosstabulation

		Fr29: Använder mig inte av applikationer jag ej känner mig förtrogen med			
		Instämmer inte	Neutral	Instämmer	Total
Fr28: Använder applikationer även om ej helt överens med användarvillkoren	Aldrig-Sällan	7	9	49	65
	Ofta-Alltid	3	3	6	12
Total		10	12	55	77

Tabell 5.6 Förtrogenhet med applikationer

Applikationerna tillåts tillfoga information på användarnas profiler efter att användarna har godkänt applikationerna (Besmer *et al.*, 2009). De får också tillgång till den personliga informationen och till vänners personliga information. Det betyder att applikationerna får tillgång till en stor mängd data som användaren inte kan kontrollera när eller om den används (Krishnamurthy & Willis, 2008). Saltzer och Schroeder (1975) påpekar vikten av att varje program ska bara hämta så mycket information som krävs för att genomföra arbetet. Applikationer är en potentiell källa till informationsläckage eftersom de kan spåra användarens aktioner och blir en än större risk i sociala nätverk som har specifika sekretessfrågor (Cutillo *et al.*, 2009; Krishnamurthy & Willis, 2008).

Med tanke på den information som Krishnamurthy och Willis (2008) menar att applikationerna har tillgång till efter att användaren har accepterat villkoren är det förundrande att inte fler är mer reserverade över vilka applikationer de lägger till. Å andra sidan kan vi konstatera att det är många som inte läser applikationernas användarvillkor (38,9%, se tabell 5.5) och därmed inte är medvetna om de risker som de utsätts för. Att applikationerna inhämtar mer information än vad som borde krävas för att fungera är något som användarna borde reagera på, varför behöver applikationerna få information om vänner och veta allt om användaren? Vi anser att applikationerna här bör följa Saltzer och Shroeders (1975) princip om att bara hämta den information som krävs för programmet.

Applikationer kan innebära en säkerhetsrisk, det menar åtminstone Krishnamurthy och Willis (2008). Vi delar denna åsikt till fullo så länge som applikationerna har rätt att hämta all information som användaren och dennes vänner har om sig själva. Det kan vara en risk mot integriteten och följas av att applikationer säljer av information till företag eller använder informationen till direkt skada. Det är av stor vikt att användaren alltid läser användarvillkoren för applikationer så att de får en medvetenhet om vad de går med på. I synnerhet när applikationernas villkor är korta och koncisa.

Vi ställer oss också förundrade över hur användare kan välja att gå med på användarvillkor de inte är överens med eller använda applikationer de inte känner sig förtrogna med. Även om detta var en mindre del av respondenterna så är det ändå viktigt att reflektera över. Vi tror att det kan vara en fråga om inställning, att användarna inte bryr sig om sin integritet på Internet. Det är ett svårt problem att komma till rätta med, men vi tror ändå att det är en fråga om upplysning till dessa användare om vilka risker de utsätter sig själva för. Då applikationers tillgång till information kan innebära både förföljelse, direkt skada, phishing och säljande av information är vår starka rekommendation att man bör tänka över ifall man litar på applikationen och att alltid läsa användarvillkoren.

Vi har ett perspektiv som fokuserar på att kunna ge rekommendationer till användare angående integritet och säkerhet på sociala nätverk. Därför ansåg vi det vara av vikt att undersöka hur användarnas egen *inställning till att alla vänner har tillgång till all den personliga informationen* i förhållande till reflektionen hos användarna när de accepterar vänförfrågningar. En korstabulering mellan dessa två genomfördes tillsammans med ett korrelationstest, dock kunde inte något samband fastställas (se tabell 5.7).

Fr11: Bra att alla vänner kan se all information * Fr25: Reflekterar över hur väl jag känner de jag lägger till som vänner Crosstabulation

Count

		Fr25: Reflekterar över hur väl jag känner de jag lägger till som vänner		
		Aldrig-Sällan	Ofta-Alltid	Total
Fr11: Bra att alla vänner kan se all information	Instämmer inte	7	34	41
	Neutral	5	9	14
	Instämmer	4	18	22
Total		16	61	77

Correlations

		Fråga 11: Bra att alla vänner kan se allt	Fråga 25: Reflekterar över hur väl jag känner de jag lägger till som vänner
Fråga 11: Bra att alla vänner kan se allt	Pearson Correlation	1	-,031
	Sig. (2-tailed)		,788
	N	77	77
Fråga 25: Reflekterar över hur väl jag känner de jag lägger till som vänner	Pearson Correlation	-,031	1
	Sig. (2-tailed)	,788	
	N	77	77

Tabell 5.7 Reflektion kring vänförfrågan i förhållande till vänners tillgång till information

Det finns enligt Lampe *et al.* (2006) två typer av användare; de som använder nätverk för att hålla kontakt med gamla bekanta och de som vill hitta nya kontakter. Användandet av nätverk är att man vill dela information med de man känner (Cutillo *et al.*, 2009). Det går att hitta kontakter via sökningar på olika nyckelord, vilka användaren ofta lämnar när de skapar sitt konto (Luo *et al.*, 2009). Vännerna får tillgång till information som namn, födelsedag, intressen, politiska åsikter osv. Informationen kan leda till att forum/grupper skapas (Joinson, 2008). Social engineering innebär att användaren luras till att lämna ut känsliga uppgifter till angriparen (Orgill *et al.*, 2004).

Vår studie visar att en majoritet (44%) ofta eller alltid reflekterar över hur väl de känner de personer som de lägger till som vänner samtidigt som de inte tycker att det är bra att alla vänner kan se all information. Det finns även de som inte reflekterar över hur väl de känner personerna som de accepterar vänförfrågan från och som anser att det är bra att alla vänner har tillgång till all den personliga informationen. Det framgår inte av vår studie vilken av Lampes *et al.* (2006) två typer som våra respondenter är, vissa kan vara social searchers och vissa kan vara social browsers. Vi anser att oavsett vilken typ man tillhör så bör man reflektera över vem man lägger till som vän. Vårt ställningstagande har grund i att riskerna för att utsättas för social engineering och data mining ökar om man har vänner på nätverket som man inte känner. Dessa vänner kan använda informationen de ser om användaren till kartläggning för att senare kunna genomföra t.ex. identitetsstöld.

Vi tror att medvetenheten hos användarna om de risker som finns på sociala nätverk är en del av varför en så pass stor del av dem har uppgett att de inte tycker det är bra att alla vänner kan se all

information. Det uppfattas genom dessa svar en önskan om att det skulle förhålla sig annorlunda, att användarna vill kunna kontrollera vad vännerna kan se.

Vi kan också konstatera att en stor del av användarna litar på att vännerna inte lägger ut olämplig information om dem (se figur 4.7) och drar slutsatsen att detta delvis grundar sig på att de reflekterar över hur väl de känner sina vänner. Genom en korstabulering av dessa frågor ger oss svaret att det delvis förhåller sig på detta vis men att många som reflekterar över sina vänner inte nödvändigtvis litar på dem (se tabell 5.8).

Fr10: Litar att vänner ej lägger ut olämplig information om mig * Fr25: Reflekterar över hur väl jag känner de jag lägger till som vänner
Crosstabulation

Count

		Fr25: Reflekterar över hur väl jag känner de jag lägger till som vänner		
		Aldrig-Sällan	Ofta-Alltid	Total
Fr10: Litar att vänner ej lägger ut olämplig information om mig	Instämmer inte	6	16	22
	Neutral	4	10	14
	Instämmer	6	35	41
Total		16	61	77

Tabell 5.8 Tillit till vänner

När *sociala nätverk säljer information* om användare till externa företag kan det betraktas som ett integritetshot för den enskilde användaren (Chen & Shi, 2009). Med detta som bakgrund frågade vi respondenterna i studien ifall de anser att sociala nätverk inte bör använda deras information utan medgivande från dem. Det ställdes även en fråga angående vilken uppfattning användaren har gällande externa företags rätt att köpa personlig information. Svaren på frågorna var för sig är intressanta men vi fann det än mer intressant att undersöka hur svaren slog ut när man korstabulerade dessa två frågor. Det vi kan konstatera är att få respondenter anser att sociala nätverk kan använda information utan tillåtelse och att meningarna går mer isär när det gäller externa företag som köper information. Närmare 13% anser att sociala nätverk inte bör använda den personliga informationen men att företag har rätt att köpa information från de sociala nätverken. Å andra sidan är det närmare 64% som är emot både användning av information utan medgivande och försäljning av information till företag (se tabell 5.9). Vi kan också konstatera att 93,5% har intresse för vad de sociala nätverken gör med deras information, det var ingen som instämde helt i att de inte bryr sig ifall nätverken säljer informationen (se figur 4.9).

Fr13: Uppfattning SN inte bör använda min info * Fr15: Uppfattning företag ej har rätt att köpa min info Crosstabulation

Count

		Fr15: Uppfattning företag ej har rätt att köpa min info			
		Instämmer inte	Neutral	Instämmer	Total
Fr13: Uppfattning SN inte bör använda min info	Instämmer inte	1	1	1	3
	Neutral	2	3	2	7
	Instämmer	10	8	49	67
Total		13	12	52	77

Tabell 5.9 Användande av personlig information

Att köpa information är ett vanligt sätt för företag att få tillgång till potentiella kunder och där kan de sociala nätverken bidra i en stor utsträckning (Chen & Shi, 2009). Nätverkens tillgång till information gör dessutom att de får ett högt värde på marknaden och vid en eventuell försäljning då kan säljas dyrt (Cutillo *et al.,* 2009). Ett nytt sätt för företag att inhämta information är genom att själva gå ut och söka informationen på de sociala nätverken istället för att köpa upp den. De sociala nätverken använder oftast informationen från användaren till att kunna förbättra servicen på nätverket och sparar ofta information även efter en användare har avslutat sitt konto. Det blir en integritetsfråga i samma ögonblick som nätverket bestämmer sig för att sälja, oavsett om det är enskild information eller hela företaget (Chen & Shi, 2009; Cutillo *et al.,* 2009).

Det är intressant att se hur användarna inte anser att sociala nätverk bör använda deras personliga information men att vissa av dessa användare ändå tycker att företag har rätt att köpa deras information från nätverken. Som Chen och Shi (2009) påpekar så finns det numer även en möjlighet för företagen att direkt söka informationen på användarnas profiler och därmed inte behöver ta kontakt med nätverket och köpa informationen. Det bör innebära att det idag finns ett stort mörkertal för hur mycket information som faktiskt används utan användarnas tillåtelse. Ett sätt för användarna att kontrollera hur mycket information som företagen kan komma åt är att begränsa informationen som de lägger upp om sig själva, alternativt ändra inställningar för att begränsa vad som visas publikt. Då vi har ställt frågor om båda dessa möjligheter gjorde vi även här en korstabulering för att undersöka hur användarna agerat idag. Det visar sig att en fjärdedel har mycket information om sig själva på profilen samtidigt som de anser att nätverken inte bör använda informationen (se tabell 5.10). Av respondenterna är det dessutom ca 18% som angett att de har mycket information om sig själva men inte anser att företagen har rätt att köpa informationen (se tabell 5.11). Däremot är det närmare två tredjedelar som anser att nätverken inte har rätt att använda informationen utan medgivande som även anger att de inte har mycket information om sig själva på nätverket (se tabell 5.10). Angående lite information på profilen

gentemot att företag inte har rätt att köpa information är det nästan 50% av respondenterna som anser detta.

Crosstab

Count

		Fråga 23: Har mycket info om mig på SN		
		Ja	Nej	Total
Fr13: Uppfattning SN inte bör använda min info	Instämmer inte	1	2	3
	Neutral	3	4	7
	Instämmer	19	48	67
Total		23	54	77

Tabell 5.10 Information ^ Sociala nätverks användning

Fr15: Uppfattning företag ej har rätt att köpa min info * Fråga 23: Har mycket info om mig på SN

Crosstabulation

Count

		Fråga 23: Har mycket info om mig på SN		
		Ja	Nej	Total
Fr15: Uppfattning företag ej har rätt att köpa min info	Instämmer inte	6	7	13
	Neutral	3	9	12
	Instämmer	14	38	52
Total		23	54	77

Tabell 5.11 Information ^ Företags rätt att köpa information

Vi kan se att många redan har tagit åtgärder mot att företag eller andra intressenter ska kunna se alltför mycket information om användarna på deras profiler. Trots detta kan det finnas en fara i hur mycket av informationen som visas för vänner. Ett företag som söker information är troligtvis inte vän med alla den söker information om, däremot har det sociala nätverket fortfarande tillgång till all information som användaren uppger, oavsett om det visas publikt eller ej. Det innebär att risken för informationsförsäljning och hotet mot integriteten fortfarande kvarstår. Frågan som ställdes till respondenterna rörde hur mycket information som visas på nätverket vilket kan innebära att det finns mer information i databaserna. Ytterligare en intressant aspekt kan vara ifall användaren har *ändrat inställningarna* för hur mycket som visas i profilen.

Av de respondenter som anser att de sociala nätverken inte bör använda den personliga informationen (67st) har närmare 60% ändrat inställningarna helt för hur mycket som visas på profilen, medan ca 39% har ändrat delvis (se tabell 5.12).

Fr13: Uppfattning SN inte bör använda min info * Fråga 21: Har ändrat inställningarna för hur mycket som visas Crosstabulation

Count

		Fråga 21: Har ändrat inställningarna för hur mycket som visas			
		Helt	Delvis	Inte alls	Total
Fr13: Uppfattning SN inte bör använda min info	Instämmer inte	0	3	0	3
	Neutral	2	5	0	7
	Instämmer	40	26	1	67
Total		42	34	1	77

Tabell 5.12 Social nätverks användning ^ Ändrat inställningar

Vi kan konstatera att de respondenter som har varit med i studien väljer att ändra inställningar och att inte visa alltför mycket i sina profiler. En vidare fundering är hur mycket de har läst/hört efter att de blev användare på sociala nätverk och därför har ändrat i efterhand. Det finns en chans (eller risk) att det ligger information kvar i databaserna även om man som användare har valt att ta bort information eller begränsat vilken information som visas i efterhand. Som Cutillo *et al.* (2009) påpekar kan sociala nätverk spara information trots att användaren avslutar sitt konto, vilket även kan innebära att trots att användaren valt att ta bort information så finns den fortfarande lagrad i servrarna. Användaren borde därför redan vid startande av ett nytt konto noga fundera över vilken information han/hon tillhandahåller nätverket då det är svårt att påverka i en senare fas.

Att berätta för användaren hur den bör agera stämmer inte alltid överens med hur användaren *vill* agera. Sociala nätverk uppmuntrar ofta användare att uppge mycket information och detta är en möjlig påverkningskälla där användaren följer uppmaningen (Joinson, 2008). Tufekci (2008) menar att användarna vill lämna ut information för att kunna ta del av så mycket som möjligt på nätverket och att detta inte är möjligt om man inte uppger en viss mängd information. Att lämna ut mycket information om sig själv kan leda till förföljelse eller kränkning. Statusuppdateringar kan avslöja vart användaren befinner sig stora delar av dagen och fotografier eller kommentarer som tas ur sitt sammanhang kan leda till utpressning (Anderson *et al.*, 2009; Gross & Acquisti, 2005).

Vår studie tog upp ämnet om att *delge nätverket mer information än vad som var obligatoriskt* och hur användaren ställde sig till detta. För att få svaren på den första frågan besvarad följde vi även upp med en kontrollfråga. Vid en korstabulering (och som även kan ses i figur 4.10)

konstaterar vi att dessa två inte är exakt lika fördelade vilket vi hade förväntat oss. Det är 40 av respondenterna som inte är intresserade av att fylla i fält utöver de obligatoriska och som bekräftar detta genom att inte instämma i det andra påståendet (se tabell 5.13). Däremot är det 11 respondenter som inte instämmer i att de vill fylla i alla fält även om vissa inte är obligatoriska och som samtidigt menar att de är intresserade av att fylla i fält utöver de obligatoriska. Den ojämna fördelningen mellan frågorna kan bero på att det i fråga 17 står att man vill fylla i alla fält, dvs ordet ”alla” kan ha påverkat respondenternas svar. Vi kan dock konstatera att många inte är intresserade av att fylla i fält utöver de obligatoriska, och vill man fylla i fält utöver dem så är det vissa fält och inte samtliga.

Fr17: Vill fylla i alla fält även om alla inte är obligatoriska * Fr18: Inte intresserad av att fylla i fält utöver de obligatoriska Crosstabulation

Count

		Fr18: Inte intresserad av att fylla i fält utöver de obligatoriska			
		Instämmer inte	Neutral	Instämmer	Total
Fr17: Vill fylla i alla fält även om alla inte är obligatoriska	Instämmer inte	11	8	40	59
	Neutral	3	7	1	11
	Instämmer	5	2	0	7
Total		19	17	41	77

Correlations

		Fråga 17: Vill fylla i alla fält även om alla inte obl.	Fråga 18: Inte intresserad att fylla i fält utöver obl.
Fråga 17: Vill fylla i alla fält även om alla inte obl.	Pearson Correlation	1	-,485**
	Sig. (2-tailed)		,000
	N	77	77
Fråga 18: Inte intresserad att fylla i fält utöver obl.	Pearson Correlation	-,485**	1
	Sig. (2-tailed)	,000	
	N	77	77

**. Correlation is significant at the 0.01 level (2-tailed).

Tabell 5.13 Vilja att fylla i icke-obligatoriska fält

Vår studie visar att användarna inte är intresserade av att fylla i alltför mycket information om sig själva vilket går emot vad Tufekci (2008) påstår. Vi gjorde ett korrelationstest för att testa sambandet mellan påståendena då vi ansåg att det borde finnas ett sådant och kan konstatera att enligt testet är de två påståendena starkt beroende av varandra. När vi ser korstabuleringen kan vi dock konstatera att så inte är fallet och testets resultat kan bero på bristen med tillräckliga svar i alla fält. Dock ger testet oss också en stark indikation att om det hade funnits tillräckligt med svar så hade det ändå funnits ett samband.

Vi tror att användarnas motvilja till att lämna ut information kan ha uppstått efterhand som man har varit aktiv på nätverket och antingen blivit utsatt för någon form av kränkning eller hört talas om folk som har blivit det. De två frågorna som ställdes är dessutom starkt begränsade då användaren inte bara visar information som står på profilen angående sin egen livssituation utan även visar information via de applikationer som används, de statusuppdateringar som görs osv. Vår uppfattning är att många användare är medvetna om de risker och hot som finns mot integriteten och säkerheten angående den påtagliga information som finns att läsa men att de möjligen inte har samma medvetenhet om att även alla de utföranden som de gör kan påverka deras integritet. Att först tänka efter om det man lägger upp är lämpligt eller om det på något sätt kan användas mot en själv eller någon i ens närhet bör anammas av alla användare på nätverken, oavsett vilken information det är som läggs upp (foton, statusuppdateringar osv.).

En fortsättning på hur mycket information man vill uppge utöver de obligatoriska fälten är huruvida användaren anser att det är viktigt att kunna påverka den information som visas på de sociala nätverken.

Enligt Cutillo *et al.* (2009) ska all information vara dold genom standardinställningar så att användaren själv får ändra vad som ska vara publikt. Skulle standardinställningarna inte vara utformade på det sättet så ska användaren åtminstone ha möjlighet att påverka inställningarna för vad som visas. Schrammet *et al.* (2009b) menar att standardinställningarna ofta är att alla får tillgång till all information och att majoriteten av användarna inte ändrar dessa inställningar.

I studien ställdes frågor kring *ändrade inställningar* och hur viktigt det är att kunna påverka den information som finns. Av respondenterna ansåg över 97% att det är viktigt att kunna påverka den information som finns tillgänglig om dem på de sociala nätverken. Av dessa har 56% ändrat inställningarna helt och ca 43% har ändrat dem delvis. Korstabuleringen visar att det endast är en av de 75 som tycker det är viktigt att kunna påverka informationen som har valt att inte ändra inställningarna för hur mycket information som visas (se tabell 5.14).

Fråga 20: Viktigt kunna påverka den info som finns om mig på SN * Fråga 21: Har ändrat inställningarna för hur mycket som visas Crosstabulation

Count

		Fråga 21: Har ändrat inställningarna för hur mycket som visas			
		Helt	Delvis	Inte alls	Total
Fråga 20: Viktigt kunna påverka den info som finns om mig på SN	Ja	42	32	1	75
	Nej	0	2	0	2
Total		42	34	1	77

Tabell 5.14 Påverkan ^ ändrat inställningar

Under kartläggningen av de tre nätverk som studien skickades ut på konstaterades att vilka inställningar som går att ändra skiljer sig åt mellan nätverken. Svårighetsgraden på att ändra inställningarna skiljer sig också. På Match.com går det till exempel inte att radera sin profil lätt även om den går att inaktivera så att den inte är synlig längre. Inställningssidorna på Facebook är svårförståeliga och det är inte alltid de ändrade inställningarna sparas till skillnad från Twitter som har tydliga formuleringar och endast ett fåtal inställningar vilket gör det mer lättöverskådligt.

Vår studie talar direkt emot vad Schrammel *et al.* (2005) säger, att merparten av användarna inte ändrar sina inställningar utan är nöjda med det skydd standardinställningarna ger. I vår studie är det precis tvärtom, majoriteten av användarna väljer att ändra inställningarna av vad som visas om dem på de sociala nätverken. Det kan bero på att utvecklingen av integritets- och säkerhetstänkandet har tagit stora kliv framåt på fem år. För tre år sedan hade Facebook 30 miljoner användare (Joinson, 2008), idag finns det fler än 400 miljoner [4]. Det betyder att för fem år sedan fanns det ännu färre användare av Facebook. Vi tror att Facebook här får statuera ett exempel, för även om sociala nätverk har funnits under en längre period och har haft många användare så är det inte förrän under senare år som det har ökat så enormt i antal användare. I och med ökningen och utvecklingen har det också kommit upp fall där media har rapporterat om risker på nätverken. Detta i samband med en generation som växt upp med datorer och är mer misstänksamma mot internet tror vi bidrar till det resultat vi får i vår studie.

Sett ur integritets- och säkerhetsperspektiv är vi något förvånade men nöjda med det resultat som studien visar. Det pekar på att användarna förstår vikten av att bara visa vad man själv känner sig bekväm med. Ett problem vi dock kan se är risken för att användarna väljer att inte ändra inställningarna om dessa är alltför komplicerade att förstå och ändra. På Twitter går det att ändra inställningarna på ett enkelt, okomplicerat sätt då det finns få inställningar som går att ändra. Det

kan paradoxalt nog vara en säkerhetsrisk att endast ha få inställningar att ändra, då man begränsar användarens valmöjligheter till vad som visas. Vi tror inte att detta är ett stort problem på Twitter då man inte interagerar på samma sätt med andra användare som man gör på t ex Facebook. Hade däremot Facebook endast haft ett fåtal inställningar som gick att ändra kunde det istället vända sig emot användaren. Vi instämmer med Cutillo *et al.* (2009) att optimalt hade varit om användaren själv hade fått välja att aktivera vilken information som skulle visas och inte att all information automatiskt är tillgängligt så som Schrammel *et al.* (2005) menar att det är idag. Eftersom så dock inte är fallet idag vill vi uppmana alla användare att kontrollera sina inställningar och att ändra det efter sina egna önskemål. Vi vill också påpeka att ju mer information som finns tillgängligt för alla användare desto högre blir integritets- och säkerhetsrisken.

5.2 Säkerhet

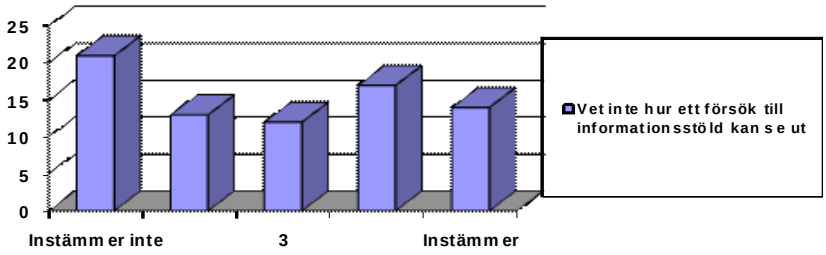
Det finns många aspekter på säkerhet som användare bör beakta när de använder sig av Internet. Valet av *lösenord* är väldigt viktigt för att säkra sina konton och information. Lösenordet bör alltid vara slumpmässigt utformat så att det inte går att gissa sig fram till det med hjälp av en användares personliga information (Chiasson *et al.*, 2009). Detta är speciellt sårbart när namn på familj, födelsedatum, husdjur med flera har använts vid genereringen. Blir lösenordet däremot för komplext kan det vara svårt att komma ihåg det. Men komplexiteten vid val av lösenord är inte den enda faktorn som kan leda till en högre säkerhet. Användaren bör dessutom använda sig av flera olika lösenord på olika konton så att om ett konto skulle bli attackerat så är inte andra i farozonen.

Vi fann genom enkätundersökningen att de flesta våra respondenter är medvetna om vikten av att använda sig av flera olika lösenord på olika ställen och de flesta av dem praktiserar också detta. (se tabell 4.2) Dessvärre fann vi att många av dem inte har helt slumpmässiga lösenord, flertalet av respondenterna använder lösenord som delvis har koppling till deras privatliv (Figur 4.14a och 4.14b). Resultatet av studien överrensstämmer väl med teorin som säger att när användare väljer lösenord är de oftast enkla och förekommer på flera olika ställen (Chiasson *et al.*, 2009; Florêncio & Herley, 2007; Mark *et al.*, 1989). Potentiellt kan detta vara en säkerhetsrisk för dessa användare.

Det är föga förvånande att användare har lösenord som har en personlig anknytning. Dessa lösenord kan vara alltför simpla och kriminella som vill utöva *social engineering* eller *data mining* kan alltför enkelt lista ut dem genom angreppsmetoderna. Vi tror att det är viktigt att användarna får förståelse för den risk de utsätter sig själva för genom att inte använda slumpmässigt genererade lösenord. Ytterligare ett problem kan då ligga i att användarna glömmer bort sina lösenord, problemet föreligger speciellt om användarna har olika lösenord till alla konton, vilket vi anser är det optimala för att skydda sin information. Vi tror att en lösning till detta kan vara att ändra t ex en känd fras till ett lösenord. ”Jag såg drottningen i London för 3 år sedan” kan bli ”JsdiLon34rs”. Vi vill dock framhäva att det viktigaste är att användaren inte

använder samma lösenord på flera konton och att användaren försöker i så stor mån som möjligt att hålla lösenorden slumpmässigt utvalda.

Förutom lösenordsval och generering av dessa ställde vi andra säkerhetsrelaterade frågor till respondenterna. Det handlade då mestadels om olika tekniker för att komma över information från användare. Till att börja med frågade vi respondenterna om de var medvetna om att de kunde utsättas för kriminella attacker på de sociala nätverken. Här hade vi en uppfattning om att det skulle vara många av respondenterna som skulle svara ja. Resultatet blev att 63,6% svarade ja och 34,6% svarade nej vilket vi blev förvånade över. Vi trodde att det skulle vara betydligt fler som var medvetna om att de kunde utsättas för detta. För att förtydliga detta fortsatte vi med att fråga respondenterna om de hade någon aning om hur ett försök till informationsstöld kan gå till.



Figur 5.1 Vetskap om informationsstöldsutförande

Det visade sig vara en ganska jämn fördelning över respondenternas kunskap om informationsstöldstekniker med något fler som visste hur det kan gå till (se figur 5.1).

Vi korstabulerade medvetenheten om dessa två frågor för att kontrollera hur stor spridningen var mellan de som var medvetna om risken för kriminella attacker och de som inte var det. Resultatet blev som förväntat att det var få respondenter som inte var medvetna om risken för kriminella attacker på sociala nätverk. Av dessa var det trots allt ett par som hade en aning om hur ett försök till informationsstöld kan gå till (se figur 5.15). Som Bilge *et al*. (2009) skriver kan även användare med ett skeptiskt förhållningssätt till säkerhet luras till att delge information vilket skulle kunna förklara att vi har respondenter som är medvetna om risken att bli utsatt men som inte vet hur ett sådant scenario kan utspela sig.

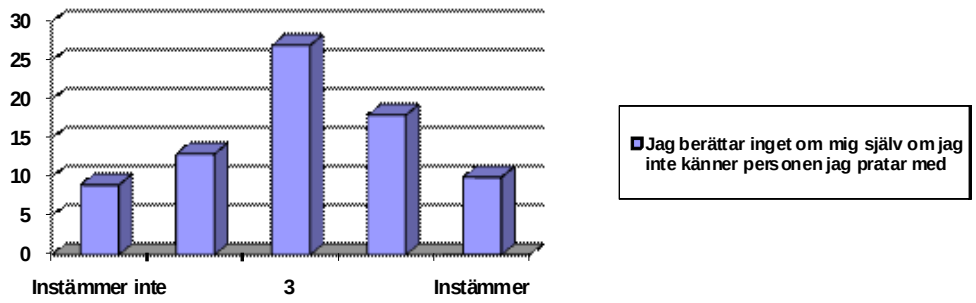
Fråga 38: Medveten om risken för kriminella attacker. * Fråga 40: Vet inte hur ett försök till informationsstöld kan gå till. Crosstabulation

		Fråga 40: Vet inte hur ett försök till informationsstöld kan gå till.					
		1 – Instämmer inte	2	3	4	5 – Instämmer helt	Total
Fråga 38: Medveten om risken för kriminella attacker.	Ja	19	10	8	6	6	49
	Nej	2	3	4	11	8	28
Total		21	13	12	17	14	77

Tabell 5.15 Medvetenhet om kriminella attacker och informationsstölder

Informationsstöld kan gå till på många olika sätt och med olika grader av teknisk komplexitet. Bilge *et al.* (2009) och Chiasson *et al.* (2009) menar att användaren är den svagaste länken ur ett säkerhetsperspektiv. En av de vanliga teknikerna för att stjäla information är *social engineering* där förövaren lurar användaren att ge ut information genom att utge sig för att vara någon annan. Ett sådant scenario kan vara att förövaren ringer upp användaren och ber om information. Vi ställde därför frågan om respondenten kunde tänka sig att ge ut personlig information till en kollega. Vår förväntan var att många av respondenterna skulle svara nej på frågan om att lämna ut personlig information till en kollega men över en tredjedel av dem svarade att de kunde tänka sig att göra det. Respondenterna fick även en följdfråga angående vad de inte skulle kunna tänka sig att ge ut. Några av respondenterna svarade då att det berodde på hur väl de kände kollegan vilket är ett bra förhållningssätt. Enligt Twichell (2006) är det just vad angriparen vill undvika genom de fyra angreppssätt de beskriver.

För att förstärka synen på hur användarna skulle reagera i ett fall av *social engineering* gav vi dem påståendet; ”*Jag berättar inget om mig själv om jag inte känner personen jag talar med*”. Här har vi fått in blandade svar där många av respondenterna inte tar ställning i frågan. Detta kan tolkas som att vissa personer inte berättar något om sig själv medan andra berättar mycket om sig själv. Merparten av respondenterna har placerat sig i mitten vilket skulle kunna innebära att de visst berättar saker om sig själv men att det är av en mer vardaglig natur som inte är så hårt knutet till det personliga livet (se figur 5.2).



Figur 5.2 Informationsutlämning

Faktumet att en del av användarna berättar (vad vi antar) personliga saker för en person som de knappt känner är oroväckande för integriteten, oavsett om det är online eller IRL. Visserligen är det även många som uppger att de inte skulle berätta personliga saker för en främling. Skillnaden skulle kunna ha sin grund i hur ens personlighet är. En person som tror alla för gott skulle kunna ge information utan att tänka på det medan en person som är lite mer vaksam mer noggrant överväger vad som sägs.

Phishing är ett sätt att stjäla information genom att angriparen skickar e-post till en stor mängd användare och hoppas på att mottagarna skall följa länkarna som bifogas. Det kan också finnas bifogade filer i e-posten som vid öppnande installerar virus i datorn (Kumaraguru *et al.*, 2007). Vi ställde respondenterna inför påståendet; ”*Jag öppnar den skräpposten som skickas till min mail*”. Hela 98,7% av respondenterna svarade att de sällan eller aldrig öppnar den skräppost som skickas till dem vilket vi ansåg vara mycket positivt (se figur 4.17). Vi tror att det kan bero på att skräppost har funnits sedan de skapade sina första e-postkonton samt att det figurerat mycket i media och således har vant sig vid/lärt sig att man inte ska öppna dem. Dock vill vi här betona att majoriteten av våra respondenter är i 20-30 års ålder. Resultatet hade kunnat se annorlunda ut om man hade haft en medelålder på 45-50 år.

En annan typ av hot som fungerar utmärkt på sociala nätverk där personer lämnar ut mycket information om sig själv är *data mining*. Data mining går ut på att angriparen kartlägger och sätter ihop små bitar av information för att få en helhetsbild av en person eller ett företag (Chen & Shi, 2009). Frågan om respondenterna tänker på möjligheten att kartlägga mina vanor på sociala nätverk finns fick resultatet att de inte gjorde det i någon högre utsträckning (se figur 4.15). Flertalet av dem svarade att de gjorde det ibland eller sällan vilket kan innebära att de förmodligen inte tycker att det som finns på deras profil är värt att kartläggas eller att de inte inser vilka följder det kan få. Skulle det vara så att användarna inte anser att det som finns på deras profil är värt att kartläggas har forskare och media en stor uppgift framför sig, nämligen att upplysa användare om att data mining kan ske genom att leta information på flera olika konton. Vi anser att det är oerhört viktigt att användaren förstår vilka konsekvenser det kan få att lägga upp information som senare inte kan raderas helt.

En av de stora nyheterna med Web 2.0 är att tredje part fick möjlighet att börja utveckla *applikationer* som sedan publicerades hos andra aktörer. Av de tre nätverk vi har undersökt är Facebook det enda av de tre som erbjuder användaren möjlighet att använda applikationer. Besmer *et al*. (2009) samt Krishnamurthy och Willis (2008) anser att det finns en risk när applikationerna får tillgång till stor mängd data som användaren inte har kontroll över. I och med att det var en facebookrelaterad fråga gavs alternativet till respondenterna att kryssa i att de inte använder Facebook men av de 77 giltiga svar vi fick in visade det sig att alla av dem använder nätverket.

Två påståenden gavs till respondenterna angående användandet av applikationer på nätverken. Den första av dem; ”*Jag är medveten om att de applikationer jag använder får tillgång till min personliga information*” (se tabell 4.4) var ett sätt för oss att kontrollera huruvida den stämde överrens med integritetsfrågan om användare läser applikationernas användningsvillkor. Av de 30 respondenter som har svarat på att de ofta eller alltid läser applikationernas användningsvillkor innan de godkänner dem, har endast 14 personer svarat att de inte var medvetna om att applikationerna får tillgång till personlig information (se tabell 5.16).

Fråga 43: Medveten om att applikationer får tillgång till personlig info * Fråga 24: Godkänner applikationers användarvillkor utan att läsa dem Crosstabulation

		Fråga 24: Godkänner applikationers användarvillkor utan att läsa dem				
		Aldrig	Sallan	Ibland	Alltid	Total
Fråga 43: Medveten om att applikationer får tillgång till personlig info	Ja	16	23	17	7	63
	Nej	4	4	5	1	14
Total		20	27	22	8	77

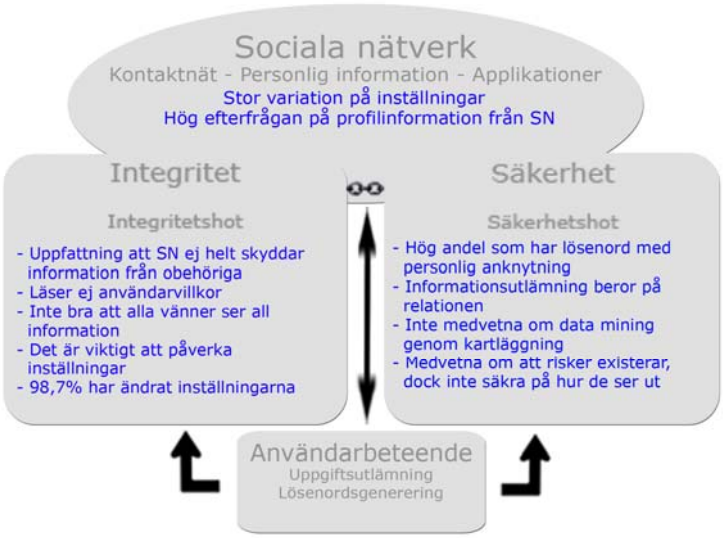
Tabell 5.16 Medvetenhet om applikationers tillgång till information

Vi drar utifrån resultatet slutsatsen att formuleringarna på dessa användningsvillkor inte alltid är så tydligt skrivna och säger bara att viss information samlas in för att kunna fungera. Något förvånande är resultatet att 24 respondenter är medvetna om att applikationer får tillgång till den personliga informationen, detta vet de trots att de ibland eller alltid godkänner användarvillkoren utan att läsa dem.

Precis som förväntat blev resultatet av nästa fråga; ”*Jag är medveten om att applikationer kan få tillgång till min personliga information genom att mina vänner har godkänt villkoren*” att betydligt färre var medvetna om detta. Endast 40,3% av respondenterna svarade ja på detta påstående (se tabell 4.4). Förmodligen beror detta på att när vännerna accepterar villkoren så

samlas informationen om vilka vänner denne har in av applikationen och ingen notis ges till berörda parter.

För att återkoppla till de begrepp som är centrala i studien och kunna få en överblick över våra resultat gjordes en kort sammanfattning som lades tillsammans med vår begreppsbild (se figur 5.3)



Figur 5.3 Resultat i förhållande till begrepp

6 Slutsats

Uppsatsen ämnar till att undersöka vilken inställning användare på sociala nätverk har till integritet och vilken medvetenhet de har till säkerhet. Detta för att kunna lämna rekommendationer åt användarna till hur de kan minska riskerna för integritets- och säkerhetshot. Frågeställningen till uppsatsen lyder:

Hur kan användare vidta försiktighetsåtgärder på sociala nätverk för att skydda sin personliga integritet och säkerhet?

Uppsatsen visar att användarna reflekterar över sin *personliga integritet* olika mycket. De läser sällan användarvillkor innan de accepterar dem men de känner sig trots detta inte helt trygga med att nätverken skyddar deras information. Användarna nyttjar applikationer trots att de ibland inte är överens med användarvillkoren eller känner sig förtrogna med applikationerna. Flera av användarna reflekterar över vilka vänner de lägger till, dock inte alltid, och meningarna kring huruvida det är bra att alla vänner kan se all den personliga informationen går isär. Det finns en gemensam tanke i att de sociala nätverken inte bör använda informationen utan att först få tillåtelse av användaren. Däremot skiljer det sig en del i frågan om företag har rätt att köpa information eller ej. Majoriteten av användarna har ändrat inställningarna för hur mycket av deras information som visas för alla användare respektive för vänner. Hur mycket information som ligger ute väger relativt jämnt mellan användarna, några har mycket och andra har lite information om sig själva. Det alla enas om är att det är viktigt att ha möjlighet att påverka vilken information som visas.

Vår uppsats visar också att användarna till viss del har insikt i de *säkerhetshot* som kan föreligga på sociala nätverk. Det är relativt jämnt fördelat mellan hur många som har lösenord som är slumpmässiga respektive personligt valda. Många av respondenterna var medvetna om att det kan förekomma kriminella attacker, dock var något färre medvetna om att det kan ske i form av socialt umgänge. Majoriteten av respondenterna visste att applikationer fick tillgång till deras personliga information, men även här var det färre som var medvetna om att applikationerna även får tillgång till vänners information.

Genom att analysera resultatet från studien i samband med vår teoretiska referensram och våra egna reflektioner har vår uppsats visat på olika företeelser där användare själva kan påverka sin integritet och förebygga att säkerhetsbrott genomförs. Utifrån dessa har följande rekommendationer utformats:

- **Läs alltid användarvillkoren.**
  Här regleras hur nätverket hanterar integritets- och säkerhetsfrågor vilket kommer att påverka dig som användare.
- **Tänk efter först om det Du vill ladda upp har ett lämpligt innehåll.**

Kan det användas mot dig? Vill du att alla (även arbetsgivare etc.) ska kunna se bilderna från festen i helgen?

- **Rensa regelbundet Din profil från oönskat material och material som Du inte längre har användning för.**
  Mycket information ger en möjlighet för angripare att kartlägga ditt liv. Finns det information som du inte längre vill visa, ta bort det!
- **Undersök vilka olika inställningar som finns tillgängliga för Ditt konto.**
  Bättre att stänga av all funktionalitet först och sedan aktivera det du vill ska vara tillgängligt än att visa mycket information som du inte känner dig bekväm med att alla ska se.
- **Granska alltid det som Du får skickat till Dig, även om det kommer från en vän.**
  Tyvärr finns det dem som hackar dina vänners konton i kriminellt syfte. Ring hellre din vän och diskutera vad som skickats till dig.
- **Läs igenom det Du skrivit ordentligt innan Du publicerar det. Tänk efter en extra gång.**
  Berättar det vart du befinner dig eller vad du gör? Kan det utgöra en risk för inbrott, förföljelse etc.?
- **Använd aldrig samma lösenord på olika konton.**
  Ju fler gånger du använder samma lösenord, desto lättare är det för en angripare att kapa dina konton. Du förhindrar dessutom angriparen från att få tillgång till flera konton om lösenorden varierar.
- **Använd lösenord som är slumpmässigt genererade.**
  Personliga lösenord är lätta att lista ut via kartläggning. Använd slumpmässigt genererade, eller se åtminstone till att ha blandat versaler, gemener och siffror i lösenordet.

Vi kan dra slutsatsen att användare kan skydda sin personliga integritet och säkerhet genom att noggrant kontrollera sin information och alltid vara uppmärksam på vilken information som tas emot. Dessutom bör användaren undvika att använda personliga lösenord och alltid ha olika lösenord på olika konton.

6.1 Framtida forskning

Vår uppsats har resulterat i en djupare förståelse för integritet och säkerhet på sociala nätverk ur användarens perspektiv samt för hur användaren kan minimera riskerna genom sitt agerande. Vidare anser vi att vidare forskning inom området med inriktning på användaren är nödvändigt. Vi tycker också att det hade varit intressant att se på liknande studier som riktar sig mot sociala nätverk för att påverka dem.

Vidare forskning som vänder sig mot användare bör studera varför användaren har en avspänd relation till integritet på sociala nätverk. Det skulle kunna ge en förståelse som kan leda till mer ingående reflektioner kring användarens beteende. Resultaten av en sådan studie skulle också kunna ligga till grund för fortsatta studier kring hur de sociala nätverken kan underlätta för användaren i integritets- och säkerhetsfrågor.

7 Referenser

WWW:

[1] Alexa the Web Information Company, URL: http://www.alexa.com/topsites/countries/SE, hämtat 2010-02-19

[2] TechWorld, URL: http://sakerhet.idg.se/2.1070/1.294051/sa-blir-du-streetsmart-pa-facebook, hämtat 2010-02-18

[3] Facebook, URL: http://www.facebook.com

[4] Facebook Pressrum, URL: http://www.facebook.com/press/info.php?statistics, hämtat 2010-02-22

[5] My Space Factsheet, URL: http://www.myspace.com/pressroom?url=/fact+sheet/, hämtat 2010-02-22

[6] Wikipedia, URL: http://www.wikipedia.org

[7] Google Calendar, URL: http://www.google.com/calendar

Artiklar:

Acquisti, A. and Gross, R., (2006) *Imagined Communities: Awareness, Information, Sharing, and Privacy on the Facebook*, Privacy Enhancing Technologies Workshop 2006

Anderson, J., Bonneau, J., Diaz, C. & Stajano, F., (2009) *Privacy-Enabling Social Networking Over Untrusted Networks*, WOSN'09, Barcelona, Spanien

Besmer, A., Richter Lipford, H., Shehab, M. & Cheek, G., (2009) *Social Applications: Exploring A More Secure Framework*, Symposium On Usable Privacy and Security 2009

Bilge, L., Strufe, T., Balzarotti D. & Kirda, E., (2009) *All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks*, World Wide Web Conference 2009, Madrid, Spanien

Brodie, C., Karat, C-M., Karat, J. & Feng, J., (2005) *Usable Security and Privacy: A Case Study of Developing Privacy Management Tools*, Symposium On Usable Privacy and Security 2005

Burke, M., Marlow, C. & Lento, T., (2009) *Feed Me: Motivating Newcomer Contribution in Social Network Sites*, CHI 2009

Chen, X. & Shi, S., (2009) *A Literature Review of Privacy Research on Social Network Sites,* 2009 International Conference on Multimedia Information Networking and Security

Chiasson, S., Forget, A., Stobert, E., van Oorshot, P.C. & Biddle, R., (2009) *Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords,* CCS'09

Couper, M. P., Tourangeau, R. & Steiger, D. M., (2001) *Social Presence in Web Surveys,* CHI 2001, Vol. 3, Issue 1

Cutillo, L.A., Molva, R. & Strufe, T., (2009) *Privacy Preserving Social Networking Through Decentralization,* Sixth International Conference on Wireless On-Demand Network Systems and Services 2009.

Danezis, G., (2009) *Inferring Privacy Policies for Social Networking Services,* AlSec'09

Flinn, S. & Lumsden, J., (2005) *User Perceptions and Security on the Web,* In the Third Annual Conference on Privacy, Security and Trust 2005

Florêncio, D. & Herley, C., (2007) *A Large-Scale Study of Web Password Habits,* WWW 2007

Gaw, S. & Felten, E. W., (2006) *Password Management Strategies for Online Accounts,* Symposium On Usable Privacy and Security 2006

Gjoka, M., Sirivianos, M., Markopoulou, A. & Yang, X., (2008) *Poking Facebook: Characterization of OSN Applications,* WOSN'08

Gross, R. och Acquisti, A., (2005) *Information Revelation and Privacy in Online Social Networks,* The 2005 ACM Workshop on Privacy in the Electronic Society

Jamali, M. och Abolhassani, H., (2006) *Different Aspects of Social Network Analysis,* Proceedings of the 2006 IEEE/ACM International Conference on Web Intelligence

Joinson, Adam N., (2008) *'Looking at', 'Looking up' or 'Keeping up with' People? Motives and Uses of Facebook,* CHI 2008 Proceedings

Kantarcioglu, M., Jin, J. & Clifton, C., (2004) *When do Data Mining Results Violate Privacy?,* KDD'04, Seattle, USA

Krishnamurthy, B. & Willis, C.E, (2008) *Characterizing Privacy in Online Social Networks,* WOSN'08, Seattle, USA

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J. & Nunge, E., (2007) *Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System,* CHI 2007, San José, USA

Kuo, C., Romanosky, S. & Cranor, L. F., (2006) *Human Selection of Mnemonic Phrase-based Passwords*, Symposium on Usable Privacy and Security 2006

Lampe, C., Ellison, N. & Steinfield, C., (2006) *A Face(book) in the Crowd: Social Searching vs. Social Browsing*, In the Proceedings of the Conference on CSCW'06

Luo, W., Liu, J., Liu, J. och Fan, C., (2009) *An Analysis of Security in Social Networks*, 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing

Maia, M., Almeida, J. och Almeida, V., (2008) *Identifying User Behavior in Online Social Networks*, Social Nets'08

Mark, T., Lomas, A., Gong, L., Saltzer, J. H. & Needham, R. M., (1989) *Reducing Risks from Poorly Chosen Keys*, ACM SIGOPS Operating Systems Review, vol. 23, 5, 14-18

Nazir, A., Raza, S. & Chuah, C-N., (2008) *Unveiling Facebook: A Measurement Study of Social Network Based Applications*, IMC'08

Orgill, G. L., Romney, G. W., Bailey, M. G & Orgill, P. M, (2004) *The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems*, SIGITE'04, Salt Lake City, USA

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., Orr, R. R., (2009) *Personality and motivations associated with Facebook use*, Computers in Human Behavior 25, 578-586

Saltzer, J. & Shroeder, M., (1975) *The Protection of Information in Computer Systems*, Proceedings of the IEEE 63 (9)

Schrammel, J., Köffel, C. & Tscheligi, (2009a) M., *How Much do You Tell? Information Disclosure Behavior in Different Types of Online Communities*, C&T'09, Pennsylvania, USA

Schrammel, J., Köffel, C. & Tscheligi, M., (2009b) *Personality Traits, Usage Patterns and Information Disclosure in Online Communities*, HCI 2009 – People and Computers XXIII – Celebrating people and technology

Squicciarini A. C., Shebab M. & Paci, F., (2009) *Collective Privacy Management in Social Networks*, WWW 2009

Strater, K. & Richter Lipford, H., (2008) *Strategies and Struggles with Privacy in on Online Social Networking Community*, Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction - Volume 1, p. 111-119

Tufekci, Z., (2008) *Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites*, Bulletin of Science, Technology and Society Vol.28 No.1

Twitchell, D. P, (2004) *Social Engineering in Information Assurance Curricula*, InfoSecCD Conference 06, Kennesaw, USA

van Oorschot, P. C. & Thorpe, J., (2008) *On Predictive Models and User-Drawn Graphical Passwords*, ACM Transactions on Information and System Security, Vol. 10, No. 4, Article 17

Walters, G. J., (2001) *Privacy and Security: An Ethical Analysis*, ACM SIGCAS Computers and Society, vol. 31, 2, 8-23

Young, A. L. & Quan-Haase, A., (2009) *Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook*, C&T'09

Litteratur:

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

Denscombe, M. (2000) *Forskningshandboken.* Lund: Studentlitteratur.

Jacobsen, D. I. (2002) *Vad, hur och varför?.* Lund: Studentlitteratur.

Kvale, S. (1997) *Den kvalitativa forskningsintervjun,* Lund: Studentlitteratur

Patel, R., Davidson, B. (1994) *Forskningsmetodikens grunder* Lund: Studentlitteratur

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

Wahlgren, L., (2005) *SPSS steg för steg* Lund: Studentlitteratur

Whitman, M. E., & Mattord, H. J. (2005) *Principles of Information Security.* Massachusetts: Thomson Course Technology.

Bilagor

Bilaga 1 - Operationaliseringsschema

Integritet			
Beteende			
Profilskapande	*Inställningar*	*Interaktionsparter*	*Interaktionstyper*
Inställningen till hur integriteten påtänks vid skapande av profil.	Inställningen till vilken information användaren vill visa.	Vilka andra parter användaren vill dela sin information med.	Användarens inställning till de olika interaktionstyper som erbjuds.
Jag tänker mycket på min personliga integritet när jag skapar nya användarkonton.	Generellt sätt är jag rätt att de sociala nätverken ska använda min information på ett sätt som gör att min personliga integritet kränks.	Jag litar på att de vänner jag lägger till inte kommer att lägga ut olämplig information om mig.	Min uppfattning är att de sociala nätverken inte bör använda min information utan min tillåtelse.
Jag tycker det är viktigt att läsa användarvillkoren innan jag accepterar dem.	Min uppfattning är att de sociala nätverken skyddar min information från obehöriga.	Jag tycker att det är bra att alla mina vänner kan se all information om mig.	Jag bryr mig inte om huruvida de säljer information om mig till andra företag.
Jag läser aldrig användarvillkoren när jag skapar en ny profil.		Jag tycker det är viktigt att fundera över vilka man väljer att lägga till som vänner.	Min uppfattning är att andra företag inte har rätt att köpa min information från de sociala nätverken.

Integritet			
Uppgiftsutlämning			
Profilskapande	*Inställningar*	*Interaktionsparter*	*Interaktionstyper*
Vad användaren lämnar ut för information vid skapande av profil.	Vilka inställningar användaren gör för att skydda sin personliga integritet.	Vilka parter användaren väljer att interagera med.	Hur användaren använder olika interaktionstyper.
Jag lämnar alltid ut mitt rätta namn vid profilskapande.	Jag tycker det är viktigt att kunna påverka hur mycket information som visas om mig på det sociala nätverket.	Jag reflekterar över hur väl jag känner de personer jag lägger till som vänner.	Jag använder applikationer även om jag inte är helt överens med användarvillkoren.
Jag vill fylla i alla fält även om vissa inte är obligatoriska.	Jag har ändrat inställningarna för hur mycket av min personliga information som visas.	Jag lägger endast till personer jag känner som vänner.	Jag använder mig inte av applikationer som jag inte känner mig förtrogen med.
Jag är inte intresserad av att fylla i fält utöver de obligatoriska.	Jag väljer noggrant ut vilken information som visas på min profil.	Jag använder mig av applikationer.	
Jag godkänner de sociala nätverkens användarvillkor utan att läsa dem först.	Jag har mycket information om mig på min profil.		
	Jag godkänner applikationers användarvillkor utan att läsa dem först.		

Säkerhet		
Lösenord	**Säkerhetshot**	**Applikationer**
	Social Engineering - Phishing - Data Mining	*Interaktionstyper*
Hur användarens lösenordsvanor ser ut.	Hur medveten användaren är om de olika säkerhetshot som finns.	Hur medveten användaren är om applikationer som informationskälla.
Mitt lösenord har koppling till mitt personliga liv	Jag ger ut information om mig själv till en kollega som efterfrågar det.	Jag är medveten om att applikationer jag godkänner får tillgång till min personliga information.
Mitt lösenord är slumpmässigt utvalt.	Jag berättar inget om mig själv om jag inte känner personen jag talar med.	Jag är medveten om att applikationer kan få tillgång till min personliga information genom att mina vänner har godkänt villkoren.
Jag är medveten om att samma lösenord på flera konton ökar säkerhetsrisken.	Jag tror att jag skulle märka om jag blev utsatt för försök till informationsstöld.	
Jag använder mig av flera olika lösenord.	Jag öppnar ofta den skräppost som skickas till min mail.	
	Jag är medveten om att den information jag visar andra kan användas till att kartlägga mina vanor.	
	Jag är medveten om att jag kan utsättas för kriminella attacker på de sociala nätverken.	
	Jag vet inte hur ett försök till informationsstöld kan gå till.	
	Jag är medveten om att attacker kan förekomma i form av social kommunikation.	

Bilaga 2a – Enkätfrågor

1. Kön
2. Ålder
3. Nätverk – med alternativ
4. Andra nätverk – öppen fråga
5. Jag tänker mycket på min personliga integritet när jag skapar nya användarkonton.
6. Jag tycker att det är viktigt att läsa användarvillkoren innan jag accepterar dem.
7. Jag läser aldrig användarvillkoren när jag skapar en ny profil.
8. Generellt sätt är jag rädd att de sociala nätverken ska använda min information på ett sätt som att min personliga integritet kränks.
9. Min uppfattning är att de sociala nätverken skyddar min information från obehöriga.
10. Jag litar på att de vänner jag lägger till inte kommer att lägga ut olämplig information om mig.
11. Jag tycker att det är bra att alla mina vänner kan se all information om mig.
12. Jag tycker det är viktigt att fundera över vilka man väljer att lägga till som vänner.
13. Min uppfattning är att de sociala nätverken inte bör använda min information utan min tillåtelse.
14. Jag bryr mig inte om huruvida de sociala nätverken säljer information om mig till andra företag.
15. Min uppfattning är att andra företag inte har rätt att köpa min information från de sociala nätverken.
16. Jag lämnar alltid ut mitt rätta namn vid profilskapande.
17. Jag vill fylla i alla fält även om vissa inte är obligatoriska.
18. Jag är inte intresserad av att fylla i fält utöver de som är obligatoriska.
19. Jag godkänner de sociala nätverkens användarvillkor utan att läsa dem först.
20. Jag tycker att det är viktigt att kunna påverka hur mycket information som visas om mig på det sociala nätverket.
21. Jag har ändrat inställningarna för hur mycket av min personliga information som visas.
22. Jag väljer noggrant ut vilken information som visas på min profil.
23. Jag har mycket information om mig på min profil.
24. Jag godkänner applikationers användarvillkor utan att läsa dem först.
25. Jag reflekterar över hur väl jag känner de personer jag lägger till som vänner.
26. Jag lägger endast till personer jag känner som vänner.
27. Jag använder mig av applikationer.
28. Jag använder applikationer även om jag inte är helt överens med användarvillkoren.
29. Jag använder mig inte av applikation som jag inte känner mig förtrogen med.
30. När jag väljer lösenord har det en koppling till mitt personliga liv.
31. När jag väljer lösenord är det slumpmässigt valt.
32. Jag är medveten om att samma lösenord på flera konton ökar säkerhetsrisken.

33. Jag använder mig av flera olika lösenord.
34. Jag ger ut information om mig själv till en kollega som efterfrågar det.
35. Om nej, vilken information kan du i sådant fall inte tänka dig att lämna ut?
36. Jag berättar inget om mig själv om jag inte känner personen jag talar med.
37. Jag tänker på att möjligheten att kartlägga mina vanor genom informationen jag lägger ut på nätverk finns.
38. Jag är medveten om att jag kan utsättas för kriminella attacker på de sociala nätverken.
39. Om ja, vilka typer av attacker känner du till?
40. Jag vet inte hur ett försök till informationsstöld kan gå till.
41. Jag är medveten om att informationsstöld kan utföras genom social kommunikation.
42. Jag öppnar den skräppost som skickas till min mail.
43. Jag är medveten om att de applikationer jag använder får tillgång till min personliga information.
44. Jag är medveten om att applikationer kan få tillgång till min personliga information genom att mina vänner har godkänt villkoren.

Bilaga 2b – Webbenkät

Integritet och Säkerhet i Sociala Nätverk

Vi är två studenter vid Högskolan i Halmstad som skriver vår C-uppsats om säkerhet och integritet i sociala nätverk. Studien har till syfte att undersöka vilken inställlning och medvetenhet till integritet och säkerhet användare har vid dylika nätverk. Med stöd av svaren vi får in av denna enkät vill vi bidra till att öka medvetenheten hos användare vid sociala nätverk.

Som respondent till denna enkät har Du varit aktiv vid ett socialt nätverk, antingen match.com, Twitter eller Facebook. Vi vill förtydliga att i de frågor som är Facebook-relaterade kan Du som inte har Facebook-profil istället välja alternativet "Använder inte Facebook".

När Du svarar på undersökningen vill vi att Du har i åtanke hur vi definierar **integritet** och **säkerhet**.
Integritet är rätten att kontrollera sin personliga information och vart den skall visas, samt att de nätverk som du väljer att lämna din information till inte får använda din information för något annat ändamål än avtalat.
Säkerhet är hur integriteten skyddas, vilka som genom teknik har tillgång till att ändra och använda informationen.

Du som respondent är helt anonym i undersökningen. Informationen som Du ger kommer att sparas i en databas, där Ditt svar tilldelas ett slumpmässigt valt ID-nummer. Du är därmed garanterad full anonymitet och vi kommer inte att kunna spåra den information vi har fått in.

Tack för din medverkan!

Madeleine Holgersson
Henrik Smederöd

Till enkäten

Integritet och Säkerhet i Sociala Nätverk

Sida 1/6

Kön

Kvinna Man

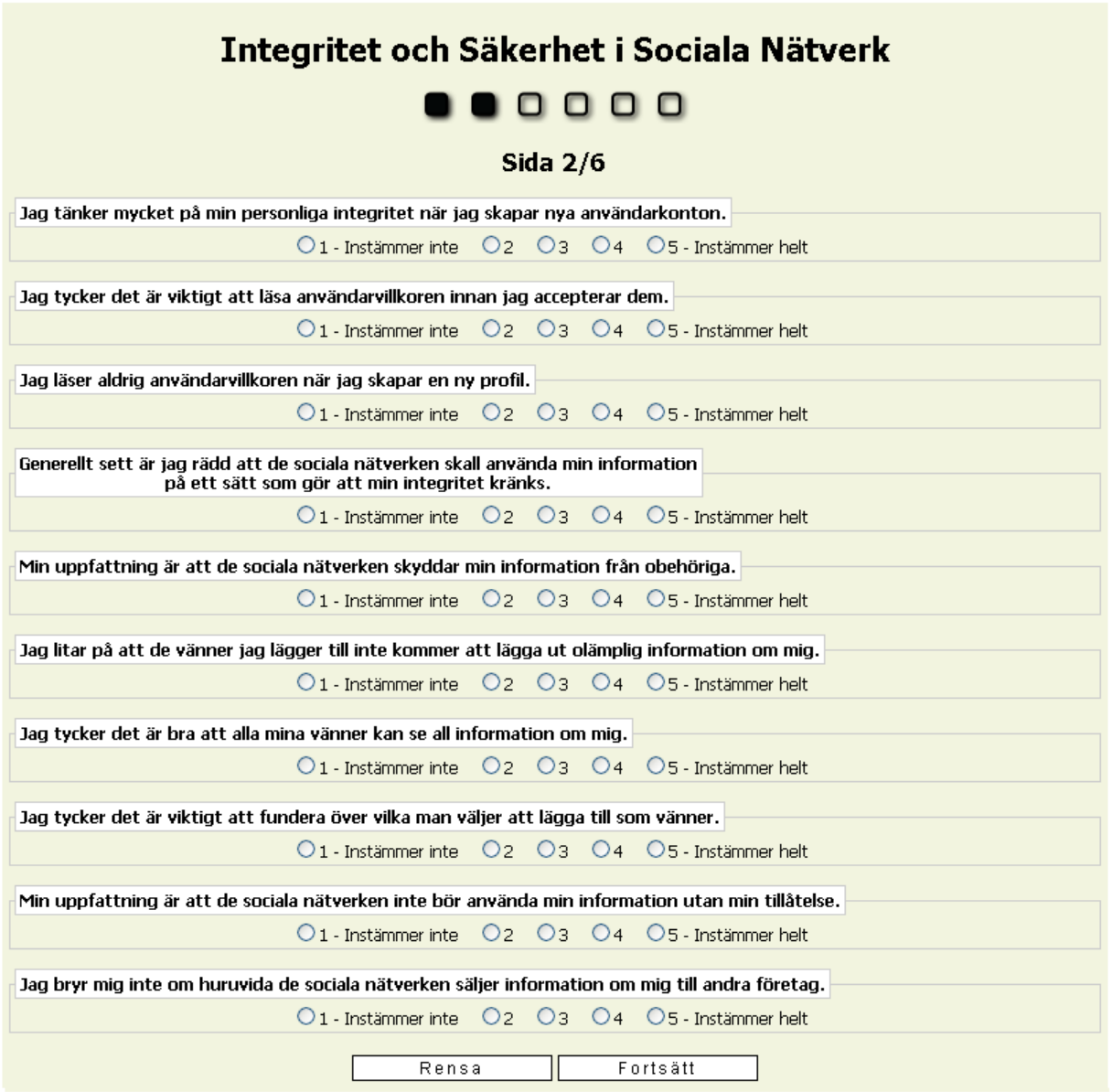
Ålder

Nätverk

Delicious Facebook Flickr I have my own blog Lunarstorm Match.com Pusha Svenska Fans Twitter Windows LIVE

Andra nätverk (komma-separera (,) vid fler än ett)

Rensa Fortsätt



Integritet och Säkerhet i Sociala Nätverk

Sida 2/6

Jag tänker mycket på min personliga integritet när jag skapar nya användarkonton.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

Jag tycker det är viktigt att läsa användarvillkoren innan jag accepterar dem.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

Jag läser aldrig användarvillkoren när jag skapar en ny profil.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

Generellt sett är jag rädd att de sociala nätverken skall använda min information på ett sätt som gör att min integritet kränks.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

Min uppfattning är att de sociala nätverken skyddar min information från obehöriga.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

Jag litar på att de vänner jag lägger till inte kommer att lägga ut olämplig information om mig.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

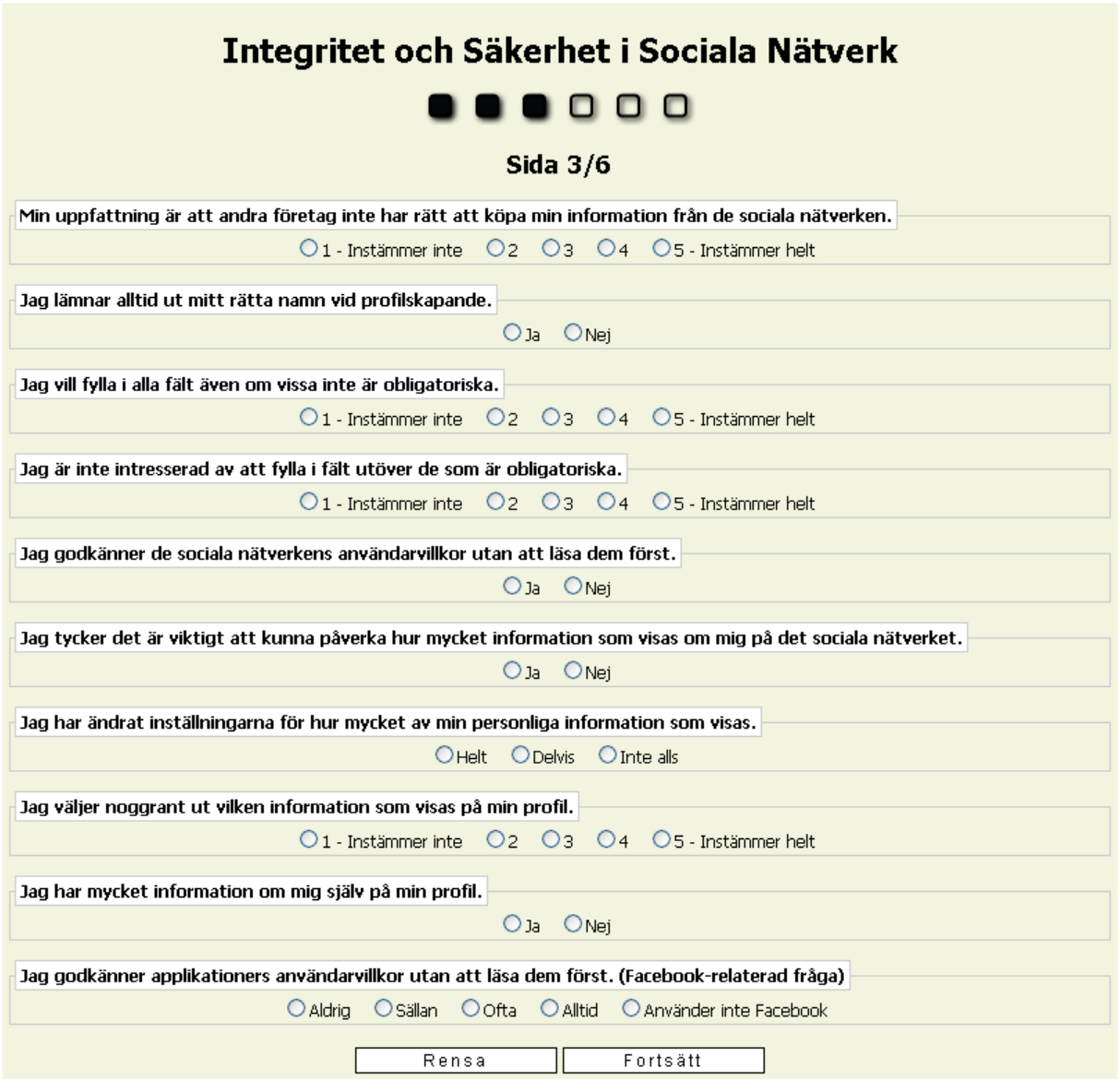
Jag tycker det är bra att alla mina vänner kan se all information om mig.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

Jag tycker det är viktigt att fundera över vilka man väljer att lägga till som vänner.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

Min uppfattning är att de sociala nätverken inte bör använda min information utan min tillåtelse.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

Jag bryr mig inte om huruvida de sociala nätverken säljer information om mig till andra företag.
○1 - Instämmer inte ○2 ○3 ○4 ○5 - Instämmer helt

Rensa Fortsätt



Integritet och Säkerhet i Sociala Nätverk

Sida 3/6

Min uppfattning är att andra företag inte har rätt att köpa min information från de sociala nätverken.

○ 1 - Instämmer inte ○ 2 ○ 3 ○ 4 ○ 5 - Instämmer helt

Jag lämnar alltid ut mitt rätta namn vid profilskapande.

○ Ja ○ Nej

Jag vill fylla i alla fält även om vissa inte är obligatoriska.

○ 1 - Instämmer inte ○ 2 ○ 3 ○ 4 ○ 5 - Instämmer helt

Jag är inte intresserad av att fylla i fält utöver de som är obligatoriska.

○ 1 - Instämmer inte ○ 2 ○ 3 ○ 4 ○ 5 - Instämmer helt

Jag godkänner de sociala nätverkens användarvillkor utan att läsa dem först.

○ Ja ○ Nej

Jag tycker det är viktigt att kunna påverka hur mycket information som visas om mig på det sociala nätverket.

○ Ja ○ Nej

Jag har ändrat inställningarna för hur mycket av min personliga information som visas.

○ Helt ○ Delvis ○ Inte alls

Jag väljer noggrant ut vilken information som visas på min profil.

○ 1 - Instämmer inte ○ 2 ○ 3 ○ 4 ○ 5 - Instämmer helt

Jag har mycket information om mig själv på min profil.

○ Ja ○ Nej

Jag godkänner applikationers användarvillkor utan att läsa dem först. (Facebook-relaterad fråga)

○ Aldrig ○ Sällan ○ Ofta ○ Alltid ○ Använder inte Facebook

Rensa Fortsätt

Integritet och Säkerhet i Sociala Nätverk

Sida 4/6

Jag reflekterar över hur väl jag känner de personer jag lägger till som vänner.
○ Aldrig ○ Sällan ○ Ofta ○ Alltid

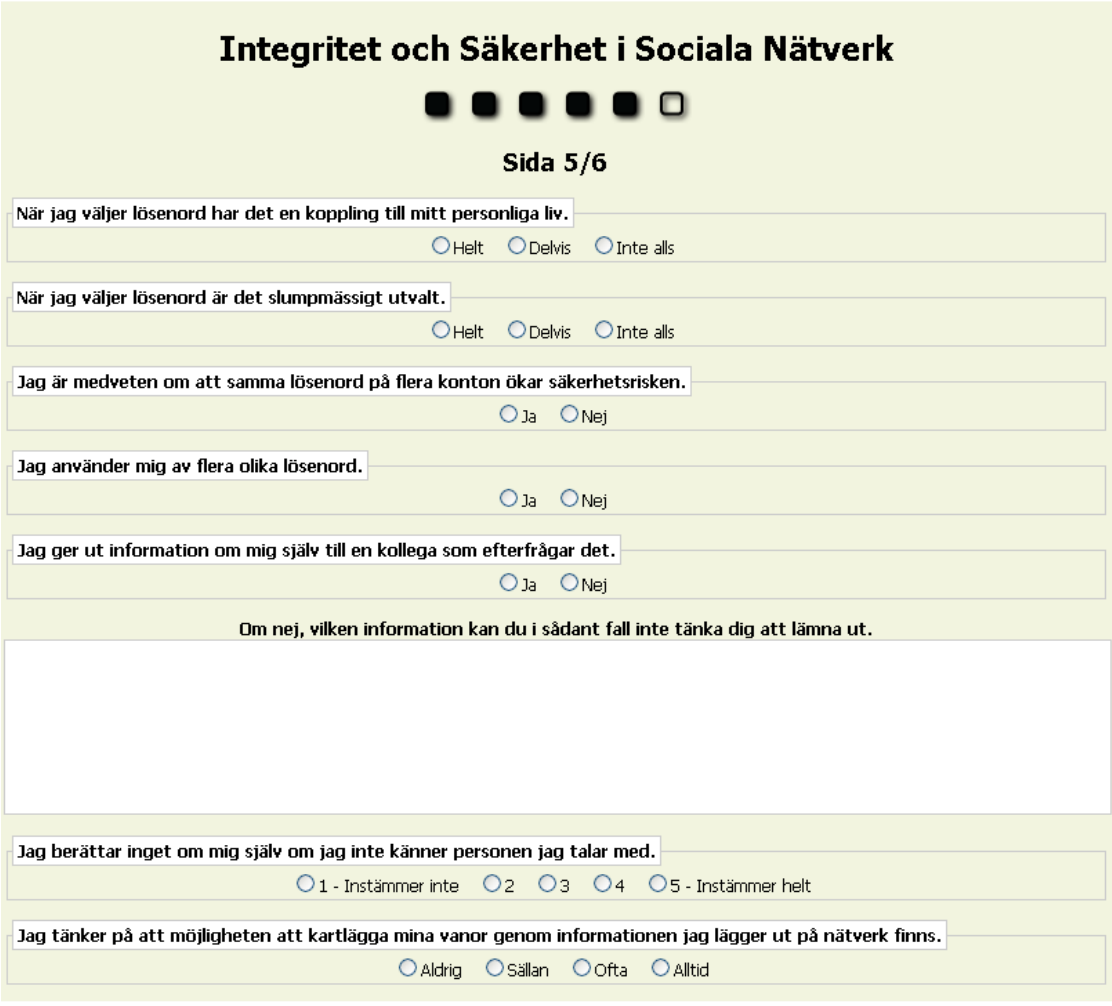
Jag lägger endast till personer jag känner väl som vänner.
○ Ja ○ Nej

Jag använder mig av applikationer. (Facebook-relaterad fråga)
○ Ja ○ Nej ○ Använder inte Facebook

Jag använder applikationer även om jag inte är helt överens med användningsvillkoren. (Facebook-relaterad fråga)
○ Aldrig ○ Sällan ○ Ofta ○ Alltid ○ Använder inte Facebook

Jag använder mig inte av applikationer som jag inte känner mig förtrogen med. (Facebook-relaterad fråga)
○ 1 - Instämmer inte ○ 2 ○ 3 ○ 4 ○ 5 - Instämmer helt ○ Använder inte Facebook

Rensa | Fortsätt



Integritet och Säkerhet i Sociala Nätverk

Sida 5/6

När jag väljer lösenord har det en koppling till mitt personliga liv.
○ Helt ○ Delvis ○ Inte alls

När jag väljer lösenord är det slumpmässigt utvalt.
○ Helt ○ Delvis ○ Inte alls

Jag är medveten om att samma lösenord på flera konton ökar säkerhetsrisken.
○ Ja ○ Nej

Jag använder mig av flera olika lösenord.
○ Ja ○ Nej

Jag ger ut information om mig själv till en kollega som efterfrågar det.
○ Ja ○ Nej

Om nej, vilken information kan du i sådant fall inte tänka dig att lämna ut.

Jag berättar inget om mig själv om jag inte känner personen jag talar med.
○ 1 - Instämmer inte ○ 2 ○ 3 ○ 4 ○ 5 - Instämmer helt

Jag tänker på att möjligheten att kartlägga mina vanor genom informationen jag lägger ut på nätverk finns.
○ Aldrig ○ Sällan ○ Ofta ○ Alltid

Integritet och Säkerhet i Sociala Nätverk

Sida 6/6

Jag är medveten om att jag kan utsättas för kriminella attacker på de sociala nätverken.

○ Ja ○ Nej

Om ja, vilka typer av attacker känner du till?

Jag vet inte hur ett försök till informationsstöld kan gå till.

○ 1 - Instämmer inte ○ 2 ○ 3 ○ 4 ○ 5 - Instämmer helt

Jag är medveten om att informationsstöld kan utföras genom social kommunikation.

○ Ja ○ Nej

Jag öppnar den skräppost som skickas till min mail.

○ Aldrig ○ Sällan ○ Ofta ○ Alltid

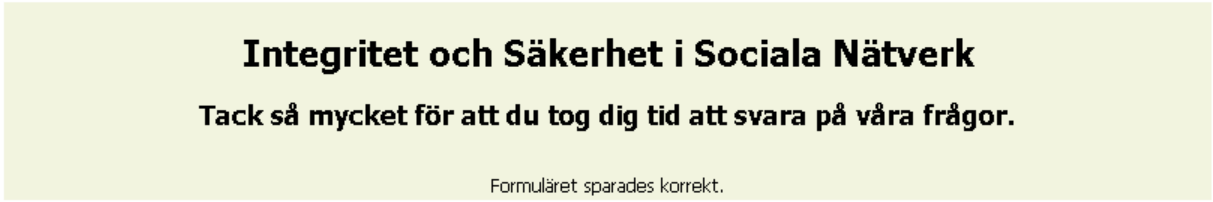
Jag är medveten om att applikationer jag godkänner får tillgång till min personliga information. (Facebook-relaterad fråga)

○ Ja ○ Nej ○ Använder inte Facebook

Jag är medveten om att applikationer kan få tillgång till min personliga information genom att mina vänner har godkänt villkoren. (Facebook-relaterad fråga)

○ Ja ○ Nej ○ Använder inte Facebook

Rensa Skicka



Integritet och Säkerhet i Sociala Nätverk

Tack så mycket för att du tog dig tid att svara på våra frågor.

Formuläret sparades korrekt.