GÖTEBORGS UNIVERSITET

# Visualisering av konton, hot och risker

## En undersökning om hur ett visualiseringsverktyg kan öka hemanvändares medvetenhet om Internetrelaterade hot och risker

## Visualization of user accounts and cyber-threats

### A study on how a visualization tool can increase home users awareness of cyber-threats

**ARAM FATEHI**
**MAGNUS LUNDIN**

**Kandidatuppsats i Informatik**

**Rapport nr. 2012:043**
**ISSN: 1651-4769**

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2012

## Sammanfattning

På senare år har allt fler hemanvändare blivit sårbara när det kommer till Internetrelaterade hot och risker. När företag och organisationer förstärker sin säkerhet blir hemanvändare allt mer intressanta som mål för bedrägerier, spam och phishing. Flera artiklar som undersökt människors kunnande och medvetenhet om Internetrelaterade hot och risker har kommit till slutsatsen att denna kunskap och medvetenhet är allt för låg, de rekommenderar därför att man forskar vidare kring detta för att hitta sätt som kan höja människors medvetenhet.

I syfte att utforska hur visualisering kan användas för att öka människors kunskap och medvetenhet om Internetrelaterade hot och risker genomför vi i denna uppsats först en kunskapsinventering kring hemanvändares medvetenhet. Vidare undersöker vi hur ett visualiseringsverktyg kan användas för att höja dessa användares kunskap och medvetenhet. Slutligen undersöks vilka aspekter inom interaktionsdesign som är viktiga att ta i bejakande när ett visualiseringsverktyg utvecklas. Undersökningen skedde i två steg, först en kvalitativ förundersökning i form av semistrukturerade intervjuer, och sedan genom en kvalitativ enkätundersökning där 38 personer deltog.

Studien bekräftar tidigare forskningsresultat som konstaterar att hemanvändares kunskap och medvetenhet om Internetrelaterade hot och risker är låg och diskuterar olika orsaker till detta. Studien visar också på att man med hjälp av visualisering kan höja kunskapen och medvetenheten hos användare, och presenterar ett antal sätt att göra detta på. Slutligen presenteras ett antal aspekter inom interaktionsdesign som är viktiga att ha i åtanke när man utvecklar ett visualiseringsverktyg, olika sätt att motivera användare till att använda verktyget.



**Nyckelord:** Visualisering, informationssäkerhet, medvetenhet, interaktionsdesign.



## Summary

In recent years more and more home users become vulnerable when it comes to cyber-threats. As companies and organizations enhance their security, home users become increasingly interesting as targets for scams, spam and phishing. Several articles that examined people's knowledge and awareness of cyber-threats and have come to the conclusion that this knowledge and awareness is too low, they recommend further research on this topic to find ways to increase people's awareness.

In order to explore how visualization can be used to increase people's knowledge and awareness of cyber-threats we perform a study about home users and awareness. Furthermore, we investigate whether a visualization tool can be used to increase the user's knowledge and awareness, and how. Finally, we explore the aspects in interaction design that are important to take in consideration when a visualization tool developed. The survey was done in two stages, first a qualitative investigation in the form of semi-structured interviews, and then through a qualitative survey where 38 people attended.

The study confirms previous research which finds that home users knowledge and awareness of cyber-threats are low, and we discuss various reasons for this. The study also shows that you can, with the help of visualization, increase knowledge and awareness among users, and proposes a number of ways how this can be done. Finally, we present a number of aspects in interaction that are important to keep in mind when developing a visualization tool, different ways to motivate users to use the tool.



**Keywords:** Visualization, information security, awareness, interaction design.

# Innehållsförteckning

# 1. Inledning

Det första steget i en forskningsprocess är att komma fram till vad man vill undersöka; det man kallar problemområdet. Ett problemområde kan uppkomma på olika sätt, det kan vara något som upplevs problematiskt men det kan också vara något som man är nyfiken på. När ett problemområde väl är valt dyker frågan upp om det verkligen finns ett behov av kunskap inom området eller om någon kommer att ha praktisk nytta av undersökningen (Davidson & Patel, 2011).

## 1.1. Bakgrund

När det gäller denna uppsats var det nyfikenhet som ledde oss till problemområdet. En diskussion vänner emellan gällande vilka lösenordsvanor vi hade och vad som egentligen kan hända när ens e-post blir hackad var startskottet för ett växande intresse för informationssäkerhet. Efter att ha gjort en mindre litteraturforskning i ämnet insåg vi att de hot och risker som användandet av Internet medför i vissa fall kan åsamka privatpersoner och företag stor skada. Denna skada är inte bara ekonomisk utan kan även komma i form av exempelvis kränkningar, hot, förföljelse och smutskastning (Kim m.fl., 2011).

När man väl satt sig in i ämnet informationssäkerhet är det också lättare att se att hackade konton, spam och phising (se avsnitt 2) är en del av de flestas vardag, både direkt och indirekt. Sedan vi började med denna uppsats har flera personer i vår omgivning fallit offer för både phishing och malware. Vi kan konstatera att vår ökade medvetenhet om Internetrelaterade hot och risker har fått oss att bli bättre på att skydda våra konton och datorer. Medvetenhet är ett genomgående tema i denna uppsats.

Hur står det då till med privatpersoners kunskap och medvetenhet gällande informationssäkerhet? Många människor säger sig förstå vilka risker och hjälpmedel som finns när det gäller Internet i stort men ser ofta inte helheten. Exempelvis att ett intrång på ett e-postkonto kan ge tillgång till ett antal andra konton eftersom e-posten oftast används av webbtjänster för att återställa lösenordet. Även individers vana att använda samma lösenord till flera olika tjänster kan utnyttjas genom att den som fått tillgång till ett konto testar samma uppgifter på flera andra konton.

Efter att ha genomfört en litteratursökning fann vi att det fanns ett antal artiklar och rapporter i ämnet som hanterade hemanvändares uppfattning av och kunskap om informationssäkerhet och Internet på olika sätt, och då denna litteratur är relativt aktuell blev det svårt att motivera en undersökning som endast behandlar medvetenhet. Den fråga som däremot återkom i mycket av litteraturen var hur man ska kunna öka hemanvändares medvetenhet och kunskap om Internetrelaterade hot och risker. Med utgångspunkt i denna fråga och den fakta som litteraturen presenterade beslutade vi oss för att gå vidare med att arbeta fram en problemformulering och ett syfte.

## 1.2. Problemformulering och syfte

I en kvantitativ undersökning från 2007 drar författarna slutsatsen att även om hemanvändare sa sig vara bekanta med säkerheten på sin dator och var nöjda med de skydd som fanns på hemdatorn, fann man att dessa datorer inte var säkra, att användarnas bristande kunskap och medvetenhet skapade en falsk trygghet. Det visade sig också att de som klassade sig som amatörer inom datoranvändning saknade det självförtroende och den kunskap som krävs för att kunna säkra sin dator (Furnell m.fl., 2007). I en kvalitativ undersökning där man intervjuade amatöranvändare av Internet konstaterar författarna att även om användare är medvetna om de hot som finns, saknar de motivation för att skydda sin hemdator. Artikeln presenterar ett antal förslag på hur man med hjälp av vissa påtvingade regler och restriktioner skulle komma förbi problemet med oskyddade hemdatorer; att ta bort användarnas ansvar helt, att på något sätt automatisera installation och uppdatering av skydd eller att inte tillåta en oskyddad dator

att komma ut på Internet alls. Författarna påpekar också att sådana förändringar skulle kräva en substantiell kulturförändring då hemdatoranvändare inte är vana vid att bli styrda och begränsade på ett sådant sätt (Furnell m.fl., 2008). I båda dessa artiklar gällande hemanvändares medvetenhet och kunskap gällande Internet och informationssäkerhet konstaterar författarna att vidare forskning inom ämnet är nödvändig, och då i synnerhet forskning om hur man kan öka individers kunskap och medvetenhet.
Vår idé är att man kan få personer att se på risker från ett nytt perspektiv genom att visualisera (se avsnitt 3) användarens konton med hjälp av ett program. Ett program som visar exempelvis användarens e-post- bank- och Facebookkonto, vilka kopplingar de har till varandra och vilka risker man då utsätts för. Detta för att öka personers medvetenhet om vilka hot som finns utan att behöva göra en litteraturforskning i stil med den vi genomfört inför denna uppsatsen.

Syftet med denna uppsats är att med hjälp av en kvalitativ förstudie och en kvantitativ enkätundersökning utforska individers Internetvanor och deras medvetenhet om Internetrelaterade hot och risker. Detta för att skaffa den information som behövs för att utreda hur man bör utforma ett visualiseringsverktyg som kan öka denna medvetenhet, och vad som är viktigt att tänka på när ett sådant verktyg utvecklas.
Uppsatsens frågeställning är:

**Hur bör ett visualiseringsverktyg som ska öka hemanvändares kunskap och medvetenhet om Internetrelaterade hot och risker utformas?**

## 1.3. Disposition

Här presenterar vi upplägget på uppsatsen. I avsnitt 2 presenterar vi ett urval av de hot och risker som Internetanvändare utsätts för. Avsnitt 3 beskriver relaterad forskning och teori, vad tidigare artiklar och uppsatser kommit fram till i ämnet. Vidare presenterar vi begreppen visualisering och interaktionsdesign. I avsnitt 4 presenterar vi ett exempel på ett program som visualiserar konton och hot, detta exempel används sedan i undersökningen. Avsnitt 5, metod, beskriver hur vi genomförde en förundersökning och en huvudundersökningen. Vi beskriver då hur vi gjort vårat urval, vilken datainsamlingsmetod som använts och hur undersökningen genomförts. Vi diskuterar även hur validiteten och reliabiliteten av undersökningsresultatet har säkerställts. I avsnitt 6 presenteras resultatet av vår enkätundersökning med hjälp av diagram. Avsnitt 7 diskuterar resultatet av undersökningen i relation till vårt syfte och vår frågeställning för att med hjälp av detta nå en slutsats. Förslag på vidare forskning följer efter det.

## 2. Hot och risker

I det som Kim m.fl. (2010) kallar ”Den mörka sidan av Internet” är alla element olagliga, oetiska eller åtminstone förkastliga, i artikeln ger de läsaren en introduktion till denna mörka sida. Med hjälp av tidigare nämnd artikel ges nu en kort introduktion till olika sätt som personer kan råka ut för obehagligheter på grund av Internet. Detta är ett urval, det finns många fler hot är dessa.

**Spam** är den stora plågan på Internet, vissa uppskattar att det skickas 200 miljarder spam om dagen. Spam kommer oftast i form av e-post, men kan också komma i form av sms, internettelefoni och instant messaging (snabbmeddelanden). Vanligtvis är spam reklam, men vissa av dem är försök till bedrägerier eller spridare av malware.

**Malware** (sabotageprogram) kommer av engelskans malicious software och är ett samlingsnamn för datorprogram som installerats på en dator utan användarens samtycke. Virus placerar sig själva på en värd i form av ett program eller en hårddisks MBR (huvudstartssektor) och sprids när värden flyttas till en annan dator. En mask är ett program som kan kopiera sig själv och sprida sig över nätverk. En Trojansk häst (Trojan horse) är ett program som på ytan ser ut att vara legitimt men som har skadlig kod gömd på insidan, kod som körs när man startar programmet. Spyware är ett malware som skickar data samlad från offrets dator, så som ekonomisk information, personuppgifter och lösenord. Adware är ett program som automatiskt visar reklam.

**Hacking** refererar till att man bryter sig in på någon annans dator. Internet har öppnat upp hackares möjligheter då man inte längre måste ha fysisk tillgång till offrets dator. Vissa hackar bara för att visa upp sin färdighet medan andra hackar för att stjäla pengar, få tillgång till känslig information, förstöra data eller för att krascha det hackade systemet.

**Denial of Service** (DoS) betyder att man översvämmar det attackerade systemet med falska förfrågningar vilket gör att systemet inte klarar av att utföra de tjänster det är meningen att det ska. DoS-attacker tar sig inte in i datorer.

**Phishing** innebär att Internetanvändare luras till hemsidor som imiterar legitima sidor; så som banker, kreditkortsföretag, Internetauktioner och sociala medier. Hemsidan försöker sen få användaren att uppge känslig information i form av exempelvis användarnamn, lösenord och kreditkortsdetaljer. Informationen kan sedan säljas vidare eller användas för att genomföra cyberbrott, stöld, identitetsstöld, bedrägeri och mycket annat.

**Klickbedrägeri** betyder att en person eller ett program genererar ett stort antal klick på en Internetannons för att antingen tjäna pengar eller för att skada annonsören ekonomiskt.

**Brott mot den digitala upphovsrätten** innebär att personer lägger upp och delar, utan tillstånd, till exempel musik, film och mjukvara. Indirekt bryter också personer mot den digitala upphovsrätten genom att dela med sig av aktiveringsnycklar och krypteringsnycklar.

**Onlinestöld** inbegriper stöld av elektroniskt kapital, data, identitet och digitala ägodelar. Onlinestöld genomförs genom att man först stjäl data i form av till exempel kreditkort, kontoinformation, användarnamn och lösenord. Stölden av data kan ha genomförts fysiskt genom att man till exempel tjuvlyssnat, letat i papperskorgar eller tagit lösenord från lappar vid personers arbetsplatser, men den kan också ha stulits med hjälp av hacking, phishing och malware.

**Onlinebedrägeri** är att lura människor att tro att de kommer att få egendom eller pengar genom att först ge bort just egendom eller pengar, sedan inser personerna att de inte fått något av värde. Onlinebedrägeri innefattar en mängd av olika sorter av bedrägerier där bedragaren i slutänden har lurat till sig till exempel pengar, kontouppgifter, kontokortsnummer eller en persons hela identitet.

**Övriga hotbilder** som användare kan komma i kontakt med är saker som cyberstalking som kortfattat innebär att man blir skadad eller förnedrad av en annan person med hjälp av Internet. Man kan via sociala medier komma i kontakt med pedofiler eller personer inom sexhandeln, och det finns till och med självmordssidor där man uppmuntrar folk att begå självmord tillsammans. Slutligen kan människor råka ut för intrång i sitt privatliv då det finns bilder och information att tillgå via till exempel sociala medier, personer kan också stjäla loggar från företag, dessa kan innehålla allt från personers sökhistorik på Internet och deras klickvanor till demografisk data.

# 3. Relaterad forskning och teori

Här presenteras först den relaterade forskningen kring hemanvändares medvetenhet om hot och risker, forskning som ligger till grund för vår enkätundersökning, därefter förklarar vi begreppet visualisering. Slutligen presenterar vi ett antal aspekter inom interaktionsdesign som är viktiga att ha i åtanke när man utvecklar ett gränssnitt eller ett program, i vårt fall en prototyp av ett visualiseringsverktyg som kan användas i vår undersökning.

## 3.1. Relaterad forskning

I en artikel från 2010 kategoriserar författarna användare av Internet som antingen home users eller non home users. En non home user använder sig av internet i arbetsrelaterat syfte, oftast på arbetsplatsen och har därför förutsättningarna att kunna använda internet på ett säkert sätt då det finns policys, guider, procedurer och utbildning inom organisationen. Ofta finns det mer eller mindre påtvingade regler och restriktioner för användning av internet. En home user, eller hemanvändare, är en person av varierande ålder och tekniskt kunnande som använder sig av internet utanför sitt arbete, och är därför själv ansvarig för att uppdatera och säkra sin dator (Kritzinger m.fl., 2010). Dessa två domäner, home user och non home user, kan överlappa varandra, men i denna uppsats är det när personer har rollen hemanvändare som diskuteras.

På senare år har allt fler hemanvändare blivit sårbara när det kommer till säkerhet och vidden av hot i allmänhet växer i en alarmerande hastighet. När företag och organisationer förstärker sin säkerhet blir hemanvändare allt mer intressanta som mål för bedrägerier, spam och phishing. Ett hemmasystem som äventyrats har potential att påverka Internetgemenskapen i stort och i slutänden påverka både företag och organisationer. När UK Department of Trade & Industry 2006 genomförde en undersökning ställdes frågan om vad som mest skulle hjälpa affärslivet att hantera risker i framtiden var det populäraste svaret, valt av 63% av de tillfrågade, att man borde utbilda allmänheten mer om informationssäkerhet och de risker som finns. Kort sagt kan organisationer bara skydda sig fullt ut om även hemanvändarna gör det (Furnell m.fl., 2007).

En undersökning som genomfördes 2006 behandlar ämnet om säkerhetsuppfattningen hos hemanvändare och ger en bra överblick över hur dessa uppfattar situationen. Redan i inledningen presenterar de resultat från en tidigare undersökning gjord i Storbritannien, och även om 87% av de som svarade tyckte att det var väldigt viktigt att skydda datorn tyckte 83% att de inte hade kunskapen som behövs för att skydda sig själv, 52% sade sig ha liten eller ingen kunskap om datorsäkerhet. Endast 15% tyckte att det var deras eget ansvar att skydda sig mot cyberbrott, 11% tyckte det var regeringens ansvar, och 49% ansåg att det var affärsvärldens och företagens uppgift. Dessa resultat tyder på att hemanvändare möter utmaningar på flera nivåer, från att de inte förstår de hot som finns och hur de fungerar till att de inte vet vart de ska vända sig när något händer. En intressant observation är att när enkäten når sin sista fråga som handlar om

ifall personerna har ändrat sina åsikter under enkätens gång, efter ett tiotal frågor om säkerhet, anser 44% att de nu är mer oroade för hot och 55% har en större medvetenhet om säkerhet och vill lära sig mer (Furnell m.fl., 2007). Detta tyder på att det inte krävs allt för mycket arbete för att göra individer uppmärksamma och intresserade av de hot och risker som Internet för med sig.
Att ämnet fortfarande är aktuellt bekräftas av att Kritzinger m.fl. (2010). Med det förslag Furnell m.fl hade till vidare forskning som underlag, presenterar de en modell för hur hemanvändare ska mer eller mindre tvingas att bli mer medvetna om de risker som finns med hjälp av en portal hos till exempel internetleverantören där man utbildas och testas innan man får tillgång till internet.

## 3.2. Visualisering

Visualisering av information beskrivs av Sharp m.fl. (2007) som ett växande fält där datorgenererade visualiseringar av komplex data är både dynamisk och interaktiv. Målet med detta är att förstärka människans kognition så man kan se mönster, trender och avvikelser. De flesta visualiseringarna är utvecklade för att man ska förstå stora mängder data som ofta är under konstant förändring. Dessa visualiseringar ger resultat snabbare än om man skulle läsa till sig den i text. Spårvagnskartor, satellitbilder och grafer är alla exempel på visualiseringar av någonting.
När det kommer till vår visualisering av konton och dess kopplingar är det just de mönster och avvikelser som beskrivs ovan som är av intresse för användaren. Även om den prototyp vi presenterar inte ska reda ut komplex data så vill vi utnyttja visualiseringens förmåga att förenkla och visa mönster för att informera människor.
Eftersom det vi ska visualisera är ett närverk av de olika konton en användare har ska vi kort beskriva detta här. Vi använder oss av vad Withall m.fl. (2007) kallar abstrakt topologisk visualisering, detta betyder att vi presenterar konton i form av noder och länkar, och att kopplingen mellan konton antingen är av eller på. Den abstrakta topologiska visualiseringen är oberoende av geografisk data och man kan då placera de olika noderna där man vill, vilket ökar synligheten. Ett sätt att göra en visualisering av nätverk tydligare är att man utnyttjar färg och storlek på noder och dess länkar (Sharp m.fl., 2007).

## 3.3. Interaktionsdesign

För att genomföra den undersökning vi tänkt krävdes också någon form av prototyp, ett program som målar upp personers konton och dess kopplingar till varandra då många troligtvis inte skulle förstå programmets syfte bara genom att man beskriver det i text. I detta avsnitt beskriver vi olika aspekter som är viktiga att tänka på när man designar en IT-artefakt (Sharp m.fl., 2007), detta för att vissa av dessa begrepp kommer att diskuteras i samband med resultatet av vår undersökning och förslag till fortsatt forskning.

### 3.3.1. Användbarhet

Användbarhetsmål används för att säkerställa att en produkt är effektiv att använda, lätt att lära sig, lätt att komma ihåg hur man använder mm., här presenteras kortfattat de användbarhetsmål som presenteras av Sharp m.fl. (2007).
**Effektivitet**, effectivity, anspelar på hur bra ett program är på att göra det som det är skapat för att göra, exempelvis att användaren har tillgång till den information som krävs och att den kan utföra sina arbetsuppgifter effektivt med hjälp av programmet.
**Förmåga att hjälpa användaren att utföra det den vill**, efficiency, syftar till att en användare ska kunna utföra det den vill med så få steg som möjligt, exempelvis genom att hemsidor minns användaruppgifter så dess besökare inte behöver skriva in

uppgifterna på nytt vid varje besök eller att ett en webbläsare har bokmärken som leder användaren till önskad hemsida via ett klick med musen.
**Säkerhet**, safety, innebär att användaren skyddas från farliga situationer och oönskade situationer. Detta kan gälla skydd från fysisk fara i form av att en tandläkare kan aktivera en röntgenmaskin från en skyddad position, men även skydd från oönskade situationer som att råka radera information och liknande. Ångra-knappar och dialogrutor som varnar är exempel på saker som gör ett program säkrare att använda.
**Nytta**, utility, betyder att ett program har den funktionalitet som krävs för att användaren kan utföra det den behöver eller vill göra, exempelvis ett bokföringsprogram som inkluderar ett beräkningsverktyg för att göra de beräkningar som krävs.
**Lätt att lära sig**, learnability, syftar till hur lätt ett program är att lära sig i relation till hur avancerat programmet är, människor är beredda att spendera mer tid på att lära sig ett avancerat program i stil med ett bokföringsprogram, men mycket mindre tid på att förstå hur man använder en DVD-spelare. Det är viktigt att fundera över hur mycket tid en användare kan vara beredd att spendera på att lära sig det program man utvecklar.
**Lätt att komma ihåg hur man använder**, memorability, anspelar på hur lätt det är att komma ihåg hur produkten används när man väl lärt sig den en gång, detta är extra viktigt när produkten används sällan. För att hjälpa en användare att minnas kan man använda sig av ikoner människor känner igen och placera dessa i rätt kategori, exempelvis att alla ritverktyg placeras på samma plats i ett ritprogram. Man ska designa för att hjälpa användaren att minnas hur man genomför uppgifter.

### 3.3.2. Användarupplevelse

Användarupplevelsen hanterar hur en användare upplever ett system, till skillnad mot användbarhetsmålen som syftar på hur användbart och produktivt ett system är ur sitt eget perspektiv. Exempel på användarupplevelsemål är känslor som tillfredsställande, spännande och roligt, men de kan också vara negativa såsom irriterande, tråkigt och frustrerande. Dessa mål är olika beroende på vad ett program är ämnat att göra, exempelvis är roligt en viktig aspekt när man utvecklar ett datorspel men inte lika viktigt när ett bokföringsprogram utvecklas (Sharp m.fl., 2007).

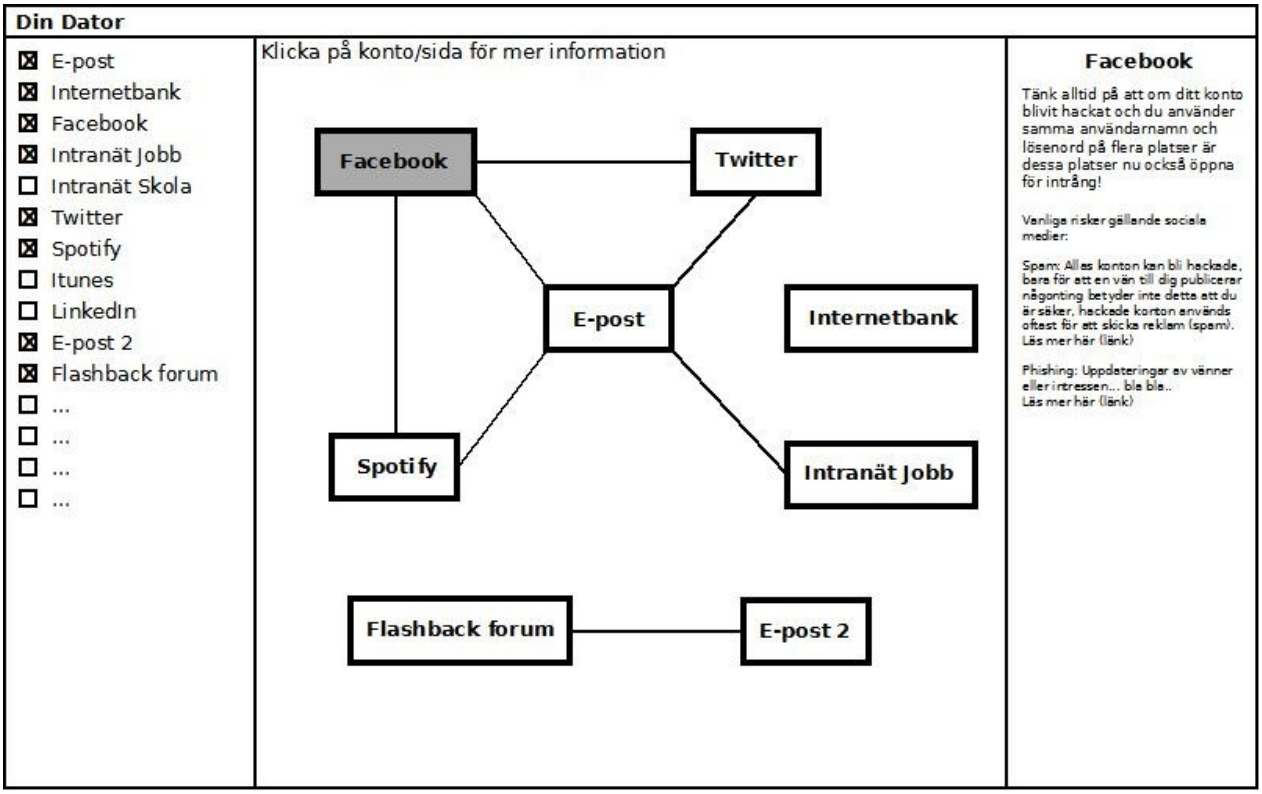
### 3.3.3. Designprinciper

Dessa principer används för att hjälpa en designer, det förklarar hur man ska tänka när man designar utifrån användarupplevelsen. Designprinciper berättar inte hur man designar något, utan de är ett hjälpmedel för att se till att man inte översett vissa aspekter i sitt program. Här presenteras de designprinciper Sharp m.fl. (2007) tar upp i sin bok Interaction design.
**Synlighet**, visibility, innebär att funktioner och knappar ska vara synliga och tydliga, att inte gömma saker i onödan. Ju mer synliga funktioner är, desto större är chansen att användaren vet vad de ska göra härnäst. Ett typiskt synligt objekt är en lysknapp, den kan bytas ut mot en rörelsedetektor, men risken är då att personer inte vet hur man släcker ljuset och det kan skapa frustration.
**Återkoppling**, feedback, handlar om att sända tillbaka information till användaren om vilken handling som utförts och vad resultatet av detta blev, och därigenom låta användaren fortsätta med sin aktivitet. Återkoppling kan ske på många olika sätt, till exempel via ljud, bild eller känsel.
**Restriktioner**, constraints, hanterar hur man hindrar användare från att utföra vissa handlingar vid det givna tillfället. Ett vanligt sätt att göra detta på i grafiska gränssnitt är att skugga vissa handlingar och därigenom göra dem omöjliga för användaren att använda vid det tillfället. En av fördelarna med restriktioner är att man skyddar användarna från att göra misstag.

**Konsekvens**, consistency, innebär i detta fall att ett gränssnitt ska vara konsekvent, att handlingar som liknar varandra även ska presenteras på ett liknande sätt. Ett konsekvent gränssnitt använder exempelvis alltid vänster musknapp för att göra val och följer de regler som andra program också styrs av; hur snabbkommandon utförs och hur man markerar allt.
**Affordance**, är ett ord som det fortfarande diskuteras om hur det borde översättas till svenska, två exempel är **uppenbarhet** och **affordans.** Detta begrepp innebär att man ska designa så att människor förstår hur man ska använda ett objekt eller ett gränssnitt, exempelvis ska ikoner bjuda in till att bli klickade på och reglage att bli skruvade på. När det gäller gränssnitt handlar det mycket om att utnyttja användarens redan inlärda konventioner.
Dessa designprinciper kan både hjälpa och stjälpa varandra och det är därför viktigt att en designer är medveten om det, exempelvis kan för mycket restriktioner minska synligheten. En designer ska också vara försiktig med att överdriva en designprincip, om man med hjälp av affordans försöker få allt i ett gränssnitt att likna fysiska objekt är chansen stor att det blir rörigt och förvirrande (Sharp m.fl., 2007).

# 4. Prototyp

För att kunna genomföra den undersökningen vi tänkt var det nödvändigt att ha ett exempel på hur ett visualiseringsprogram skulle kunna se ut, och därför valde vi att skissa upp ett fiktivt program som intervjupersonerna kunde relatera och ställa frågor kring. Denna prototyp användes alltså som en del av vår metod och är inte ett resultat av vår undersökning. Vi valde att skapa en gränssnittsskiss, i denna uppsats kallad prototyp eller visualiseringsverktyg. En gränssnittsskiss används oftast för att presentera och utveckla visioner med hjälp av andra, oftast en designgrupp (Löwgren & Stolterman, 2004), vi valde att använda denna skiss i både förundersökningen och enkätundersökningen för att få svar på vissa delar av vår frågeställning. För att denna prototyp skulle vara lätt att förstå använde vi oss av konsekvens och affordans gällande interaktionsdesign, detta innebar att vi försökte använda oss av de konventioner och den layout som många andra gränssnitt har. Figur 1 visar gränssnittsskissen.




*Figur 1: Den gränssnittsskiss som användes i undersökningen.*

Den information angående gränssnittsskissen som medföljde i enkäten och som också användes i förundersökningen presenteras här nedan:

*”Denna bild föreställer ett program som till vänster låter dig själv välja de konton du har. Du får då upp dessa konton och dess kopplingar i mitten, där du då kan klicka på dem för att få mer information om vad du borde tänka på när du besöker sidan. Där får du även kortfattad information om vanliga hot, till exempel spam, phishing och hacking.”*

Vi är av åsikten att denna information var tillräcklig för att de som deltog i intervjuerna och enkäten skulle förstå de grundläggande funktionerna i det föreslagna programmet och därför kunna besvara de frågor vi ställde.

# 5. Metod

I detta avsnitt förklarar vi vilka datainsamlingsmetoder som använts, hur vi gjort vårt urval, hur vi säkerställt reliabilitet och validitet för att slutligen beskriva genomförandet av undersökningarna. För varje rubrik kommer vi först att presentera förundersökningen och sedan huvudundersökningen.

## 5.1. Datainsamling

För att kunna utforma och testa en enkät till den huvudsakliga undersökningen genomfördes, som förundersökning, ett fåtal kvalitativa semistrukturerade intervjuer. Patel och Davidson (2011) beskriver att syftet med kvalitativa intervjuer är att ”upptäcka och identifiera egenskaper och beskaffenheten hos något, t.ex. den intervjuades livsvärld eller uppfattningar om något fenomen” (s 82). Det vi ville få ut av dessa intervjuer var hur den prototyp vi designat uppfattades av olika användare och om de frågor vi formulerat gick att förstå, slutligen ville vi också få förslag på nya frågor som kunde vara relevanta. Denna undersökning var också en del i att försöka säkerställa reliabiliteten och validiteten hos enkätundersökningen.
Huvudundersökningen genomfördes med hjälp av en enkät med fasta svarsalternativ vilket innebär att vi utgår från kvantitativt inriktade metoder. Att kvantitativt bearbeta ett resultat innebär att man med hjälp av statistik ordnar, beskriver, bearbetar och analyserar data. Typen av statistik vi använder oss av är den deskriptiva statistiken, den används för att i siffror beskriva det insamlade materialet (Patel & Davidson, 2011) En fördel med kvantitativ data är att den kan föras in i en databas och sedan filtreras, detta innebär att man lätt kan se hur till exempel en viss åldersgrupp eller personer med en viss utbildning har svarat på en eller flera frågor (Sharp m.fl., 2007). Orsakerna till att vi valde denna datainsamlingsteknik var att vi tidigt insåg att frågor som behandlar informationssäkerhet och människors kontovanor kan vara känsliga, och därför borde undersökningen vara helt anonym. Vi tog också beslutet att endast använda oss av en pappersenkät då det fanns en risk att människor skulle vara misstänksamma mot en webbenkät och att vi på så vis skulle få in alldeles för få eller felaktiga svar.

## 5.2. Urval

Till förundersökningen valde vi att intervjua tre personer, det viktiga var att de hade olika yrkesroller och olika stor erfarenhet av Internet och datorer. Här beskrivs de tre personerna kortfattat:

1. Student med lång erfarenhet av Internet och datorer, men ingen stor uttalad kunskap om de hot och risker som Internet medför. Använder Internet mest för studier, spel och film. Intervjuades i sitt hem.
2. Informationssäkerhetskonsult på ett större internationellt IT-företag. Lång erfarenhet av Internet och datorer och använder Internet flitigt både till arbete och nöje. Intervjuades på sin arbetsplats.
3. Förman på en medelstort företag. Liten erfarenhet av Internet och datorer och liten kunskap om informationssäkerhet. Använder Internet på jobbet och vid enstaka tillfällen i hemmet. Intervjuades på ett café.

Eftersom enkäten till huvudundersökningen handlar om hemanvändares medvetenhet ville vi få in svar från en så varierad undersökningsgrupp som möjligt, en undersökningsgrupp som representerar befolkningen i allmänhet. Vi valde att dela ut enkäten på ett serviceföretag, ett industriföretag och även till 6 stycken utvalda personer. Serviceföretaget har ca 500 anställda i blandad ålder och med varierad utbildningsnivå. Industriföretaget består av ca 50 anställda och även här är det stor variation på ålder och utbildning. De specifikt utvalda personerna som fick enkäten valdes för att de hade hög utbildning eller hög ålder, detta för att använda oss av deras svar om dessa grupper

skulle bli underrepresenterade i undersökningen. Vår förhoppning var att få in minst 40 besvarade enkäter.

## 5.3. Reliabilitet och Validitet

Vi kommer nu att förklara begreppen validitet, att vi undersöker det vi avser att undersöka, och reliabilitet, att vi undersöker det på ett tillförlitligt sätt (Patel & Davidson, 2011).

### 5.3.1.Validitet inom kvalitativa studier

Inom kvalitativ forskning är dessa två begrepp sammanflätade och därför använder kvalitativa forskare sällan begreppet reliabilitet. Man använder sig istället av uttrycket validitet, som då får en vidare innebörd inom kvalitativ forskning. Det är svårt att entydiga regler för hur man säkerställer validiteten i en kvalitativ undersökning; att beskriva hela forskningsprocessen noga från början till slut är ett sätt att stärka validiteten i ett kvalitativt forskningssammanhang (Patel & Davidson, 2011). Genom att beskriva vårt tillvägagångssätt tydligt och genom att vara noga med att inte försöka påverka intervjupersonerna anser vi att vi har stärkt validiteten tillräckligt gällande denna förundersökning.

### 5.3.2. Validitet

Validitet innebär att vårt instrument, i detta fall vår datainsamlingsmetod, faktiskt mäter människors medvetenhet om Internetrelaterade hot och risker, och att den också mäter om man med hjälp av visualisering kan öka denna medvetenhet. Patel och Davidson (2011) beskriver två sätt att säkerställa validitet; innehållsvaliditeten och den samtidiga validiteten.

**Innehållsvaliditet** kan man säkerställa genom att man logiskt analyserar sitt instrument och kopplar denna analys till den teoretiska referensramen. Detta innebär att man översätter teori och relaterad forskning till relevanta frågor i en enkät eller en intervju. Man kan också låta någon som är insatt i problemområdet granska instrumentet.

**Samtidig validitet** innebär att man jämför utfallet på sitt instrument med ett kriterium och på så sätt säkerställer validiteten. Detta innebär att man exempelvis kan pröva instrumentet på en annan grupp som liknar den faktiska undersökningsgruppen eller att man använder sig av andra tekniker för att ha något att jämföra med, att man jämför en enkät med intervjuer eller liknande. Man kan också använda sig av andra kriterier, till exempel statistiska uppgifter.

Vi har försökt att säkerställa validiteten genom att i första hand använda oss av den relaterade forskning vi har för att utforma frågor som besvarar det vi är intresserade av i relation till relaterad forskning. Vi har också använt oss av en förstudie för att på så vis reda ut de oklarheter som skulle kunna innebära att vi genomför en felaktig undersökning. Att inkludera frågor om kön, ålder och utbildning är också av vikt för validiteten då vi ville ha en så blandad undersökningsgrupp som möjligt, utan dessa frågor fanns möjligheten att vi av misstag undersökte exempelvis 20-åringars medvetenhet om Internetrelaterade hot.

### 5.3.3. Reliabilitet

Begreppet reliabilitet innebär att instrumentet man använder sig av är tillförlitligt, att det motstår slumpinflytanden av olika slag. Patel och Davidson (2011) förklarar att när man använder sig av en enkät har man minst möjlighet att kontrollera tillförlitlighet i förväg, man måste vara noga med att frågor är uppställda på ett bra sätt, att instruktionen till enkäten är tydlig och att frågorna i enkäten inte går att missuppfatta. Ett sätt att försöka säkerställa reliabiliteten gällande en enkät är att testa den på vänner eller kollegor innan man genomför sin undersökning. Egentligen vet man inte om en enkät är reliabel förrän

efter undersökningen är genomförd, då man kan se om personer exempelvis hoppat över frågor, markerat för många alternativ eller lagt till egna alternativ.
Även när det gäller reliabiliteten var förundersökningen till stor nytta. Genom att testa enkäten på denna grupp och att ha möjligheten att diskutera kring den, lyckades vi rätta till ett antal felaktigheter i form av hur frågorna var uppställda och att de var oklara. Även den den information som presenterar prototypen förtydligades. Vi utökade instruktionen till enkäten så det var tydligare vad vi var ute efter och förklarade också att frågor som väckte misstänksamhet, exempelvis kön och ålder, var med för att säkerställa validiteten.
När undersökningen väl genomförts kunde vi komma fram till att det endast var några enstaka personer i undersökningsgruppen som låtit bli att kryssa för något svarsalternativ på en fråga. Eftersom de det inte rörde sig om samma frågor gick det inte att urskilja någon fråga som uppfattades som otydlig eller av annan orsak inte besvarades. Vi anser därför att undersökningen är reliabel.

## 5.4. Genomförande

Intervjuerna som genomfördes i förstudien var semistrukturerade och pågick under cirka 30 minuter med en person i taget. Fem öppna frågor ställdes där intervjupersonen var helt fri att diskutera och komma med åsikter om enkäten och prototypen, vårt mål var att intervjun skulle likna ett vanligt samtal där man frågar, förklarar och diskuterar. Intervjuerna dokumenterades genom anteckningar på enkäten, prototypen och också med hjälp av ett anteckningsblock.
Intervjupersonerna introducerades till vad enkäten och vår uppsats handlade om, sedan fick de enkäten. Efter detta ställdes följande frågor:

1. Läs igenom denna enkät. Är det några frågor du inte förstår, som du tycker borde omformuleras eller som du tycker borde tas bort helt?
2. Saknar du några frågor, är det något du skulle tycka vara intressant att veta när det kommer till informationssäkerhet?

Efter att dessa frågor diskuterats visade vi en bild på den prototyp som presenterades i definitionsavsnittet och förklarade hur det var tänkt att programmet skulle fungera, sedan ställdes dessa frågor:

3. Vad är dina tankar kring detta program, förstår du det? Varför/varför inte?
4. Skulle du tycka att det vore intressant att testa ett program som detta? Varför/varför inte?
5. Finns det något du skulle vilja lägga till, ta bort eller förändra på denna bild?

Enkäten som användes i huvudundersökningen skickades endast till ett fåtal människor personligen, dessa personer fick förutom instruktionen som bifogas med enkäten en kortare förklaring till varför just deras medverkan kunde vara av vikt för vår undersökning. Största delen av enkätundersökningen genomfördes genom att vi kontaktade de två företagen för att få tillstånd att genomföra undersökningen. Vi var noga med att påpeka att det var i rollen som hemanvändare som personerna skulle svara och att företagen inte på något sätt skulle utvärderas, vi bifogade enkäten för att understryka just detta. När företagen beviljat att använde oss av dem för att nå ut med undersökningen underrättades de anställda via e-post att denna enkät skulle finnas i fikarum och lunchrum i början av maj. De anställda informerades ännu en gång när enkäterna fanns på plats och det förtydligades också att enkäten var frivillig och helt anonym. Den 10:e maj samlades enkäterna in och vi hade då sammanlagt 38 besvarade enkäter, vi kommer i avsnittet diskussion att reflektera över hur vi skull ha

kunnat få in fler svar. Svaren fördes över till en databas för att presenteras i form av grafer. Ett fåtal frågor valdes också ut för att relateras till varandra, detta för att få svar på delar av vår frågeställning, till exempel om visualiseringsverktyget var intressant för de som ansåg att de hade liten kunskap om Internetrelaterade hot och risker. Dessa jämförelser kommer att presenteras i resultatavsnittet.

# 6. Resultat

Vi kommer nu att presentera resultatet av förs förundersökninngen och sedan huvudundersökningen.

## 6.1. Förundersökning

Då detta var en förundersökning kommer vi inte att fördjupa oss i vad som sades under intervjuerna. Värt att tillägga är att vi fick information som på olika sätt kan relateras till resultatdiskussionen i avsnitt 7, och därför kommer vi i det avsnittet inte bara relatera till den kvantitativa data vi samlat in, utan även till påståenden och åsikter som framförts under dessa intervjuer.

Vi fick ett fåtal påpekanden om oklara formuleringar och någon enstaka felstavning, detta korrigerades innan enkäten skickades ut. Två personer ifrågasatte frågorna angående ålder och kön, detta för att de inte gillade tanken på att man skulle peka ut exempelvis äldre människor eller kvinnor som omedvetna eller okunniga. Med risk för att en sådan uppfattning skulle få personer att inte vilja svara på enkäten beslutade vi att i missivet, brevet som medföljer enkäten, tydligt framföra att den informationen endast ska användas för att fastställa att man fått en så varierad undersökningsgrupp som möjligt. Intervjupersonen med mest erfarenhet av Internetrelaterade hot och risker kom med ett antal förslag på frågor man skulle kunna lägga till. Flera av dessa var något för avancerade för att passa in i just denna undersökningen, men två av förslagen inkluderade vi; Vilket operativsystem man använder och hur man loggar in i Windows, förutsatt att det är operativsystemet man använder sig av.

Det fanns ett antal frågor och diskussioner som gav oss svar på *om* verktyget kunde användas för att höja medvetenhet och kunskap. Vi fann att det i prototypen fanns två stycken ”väckarklockor”; konstateranden som direkt ökade intervjupersonernas intresse av programmet och informationssäkerhet. Det första var att om en persons e-post blir hackad kan den som hackat kontot i vissa fall komma åt eller ta över alla konton som e-posten är kopplad till. Det andra konstaterandet var att alla konton som ritats upp i programmet är utsatta för risk om exempelvis spyware installerats på datorn, oavsett om de är kopplade till varandra eller inte. Efter att intervjupersonerna fått den informationen ökade deras intresse markant kring programmet och hur det kunde gå till när man blir hackad, de blev också mer intresserade av vilka risker olika hemsidor förde med sig och hur malware, virus, phishing med mera fungerar. Två av intervjupersonerna uttryckte att de inte visste vad vissa hot var, men då vi förklarade dessa visade det sig att de visste att dessa hot fanns, men de visste inte att det hette exempelvis phishing eller spyware.

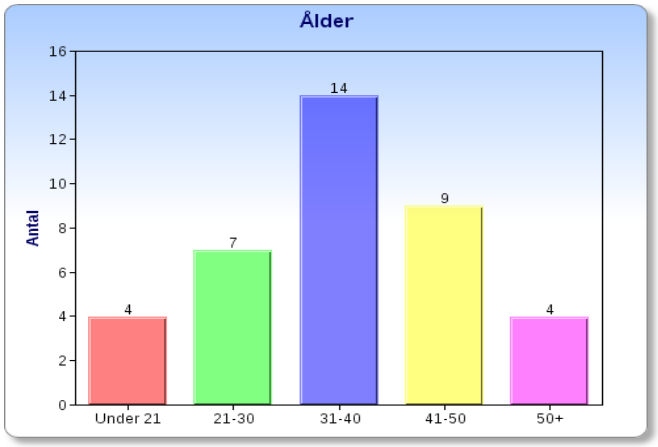
När det kommer till design och användbarhetsmål är det självklart viktigt att man har alla dessa i i åtanke när man utvecklar ett visualiseringsverktyg. En kommentar från den minst erfarne användaren av Internet förklarade bra hur viktigt det är att verktyget hjälper användaren:

*”Jag vill bara kunna klicka på lite konton jag har och se vad som händer, jag vill inte rita kopplingar, jag vill inte leta efter information, jag vill bara att programmet visar för mig varför detta kan vara farligt. Och kanske lite information om hur man skyddar sig, inget annat.”*

## 6.2. Huvudundersökning

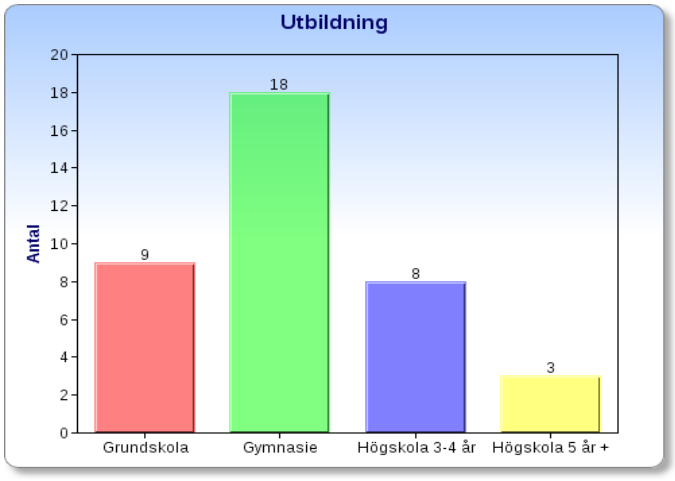
Vi kommer nu att presentera resultatet av huvudundersökningen i den ordning frågorna ställdes i enkäten. Eftersom undersökningen har färre än 50 svarande väljer vi att presentera resultatet i form av antal svarande istället för procent, efter rekommendation av Patel och Davidson (2011). De frågor som har färre än fyra svarsalternativ kommer att presenteras i text och i de fall svarsalternativen är fler presenteras resultatet också med hjälp av grafer.

De tre första frågorna i enkäten var till för att säkerställa att det var en stor variation gällande kön, utbildning och ålder i undersökningsgruppen. Av de 38 som svarat på enkäten var 20 kvinnor och 18 män, vilket ger en bra variation. Tabell 1 visar åldersfördelningen bland de svarande.



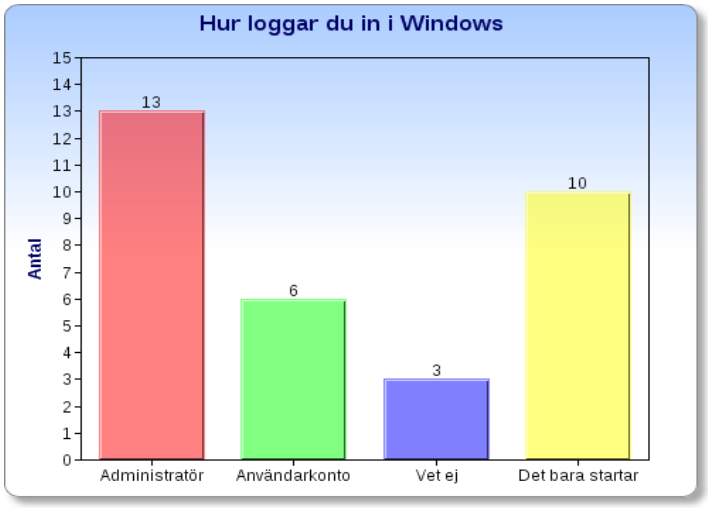

*Tabell 1: Tabell över åldersgrupperna i undersökningen.*

Gällande utbildningsnivån hos undersökningsgruppen, tabell 2, svarade 9 att de endast gått ut grundskolan, 18 att de gått ut gymnasiet, 8 svarade att de hade 3-4 år på högskola och 3 personer hade gått 5 år eller mer på högskola.



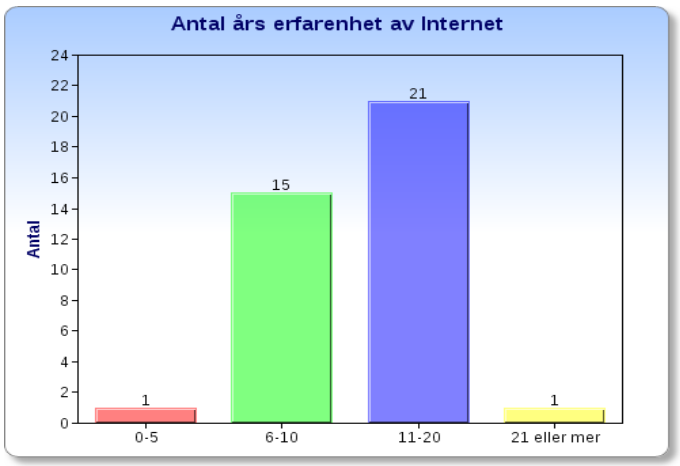

*Tabell 2: Tabell över undersökningsgruppens utbildningsnivå.*

På frågan om vilket operativsystem personerna hade på sin hemdator svarade 32 att de hade Windows och de övriga 6 att de hade Mac Os. Alla tillfrågade visste vilket operativsystem de hade och ingen valde att kryssa i alternativet annat. Att få in ett antal enkäter som besvarats av personer med en Mac är av intresse eftersom dessa personers uppfattning om säkerhet kan skilja sig från dem som har Windows, detta behandlas i diskussion.
27 av de tillfrågade svarade att deras hemdator användes av flera personer, övriga 11 datorer användes bara av en person. Detta resultat är av intresse för vissa av de frågor som diskuteras i senare avsnitt.
När frågan ställdes om hur de som hade Windows loggade in på sin dator svarade 13 att de loggade in som administratör, 6 svarade användarkonto, 3 visste inte och 10 svarade att operativsystemet bara startar. Resultatet presenteras i tabell 3.



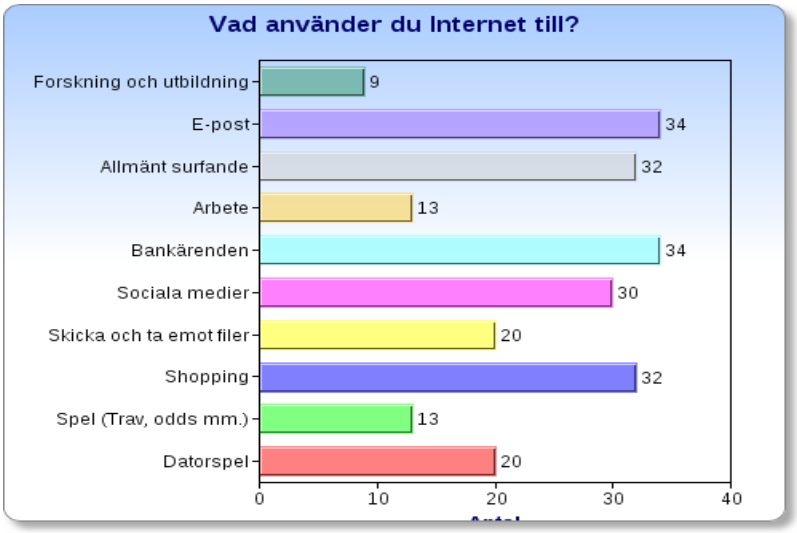

*Tabell 3: Tabell över hur de svarande loggar in i Windows.*

11 av de som loggade in som administratörer och alla som svarade att operativsystemet bara startade hade också svarat att deras hemdator används av flera personer.
När det kommer till frågan om hur många år de tillfrågade hade använt sig av Internet var det endast en person som använt sig av det i 0-5 år, och en person som svarade 21 år eller mer, de andra valde alternativen mellan dessa. 15 personer hade använt Internet i 6-10 år och 21 personer svarade att de använt sig av Internet i 11-20 år. Se tabell 4.



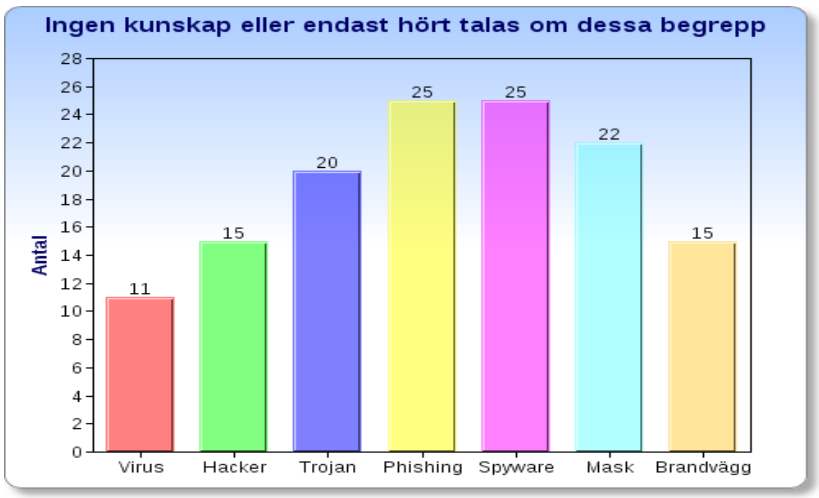

*Tabell 4: Tabell över hur många års erfarenhet av Internet underökningsgruppen hade.*

På frågan om hur mycket kunskap om Internet och datorer personen själv tyckte att den hade svarade en majoritet, 29 st, att de ansåg sig ha medelstora kunskaper. 6 personer ansåg att de hade liten kunskap och 3 personer sade sig ha mycket goda kunskaper.
När vi ställde frågan om vad personerna använde Internet till var svaren av stor variation, de alternativ som fick över 30 svar var E-post, Allmänt surfande, bankärenden, sociala medier och shopping. Det som undersökningsgruppen använde Internet till minst var spel, arbete och forskning och utbildning. Se tabell 5.



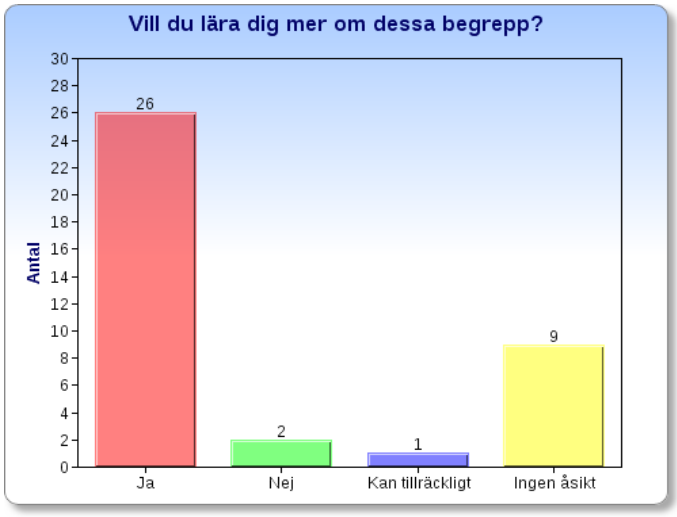

*Tabell 5: Tabell över vad de tillfrågade använder Internet till.*

Vi ställde sedan frågan om vilken kunskap personerna ansåg sig ha gällande ett antal begrepp som handlar om hot och säkerhet, svarsalternativen var ingen kunskap, hört talas om, medelkunnig och goda kunskaper. Begreppen vi frågade om är de som tabell 6 presenterar. Vi har i denna figur valt att slå samman de som svarat att de inte har någon kunskap med de som endast hört talas om dessa begrepp, detta innebär att de personer som inte innefattas i denna tabell ansåg sig ha medel eller goda kunskaper om begreppen.



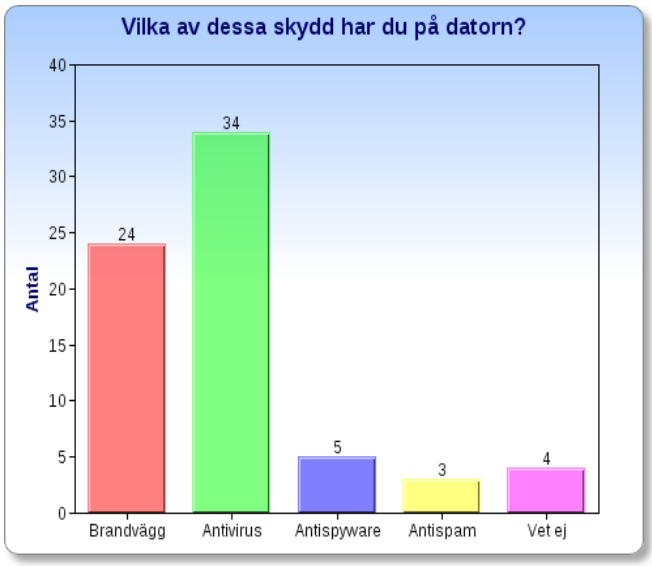

*Tabell 6: Tabell över hur många som ansåg sig endast ha hört talas om, eller inte hade någon kunskap om dessa begrepp.*

Nästföljande fråga var om personerna ville lära sig mer om de begrepp de just svarat på frågor om. 26 personer svarade ja, 2 svarade nej, 9 hade ingen åsikt och 1 person ansåg att den redan kunde tillräckligt, resultatet presenteras i tabell 7.




*Tabell 7: Tabell över undersökningsgruppens vilja att lära sig mer om tidigare nämnda begrepp.*

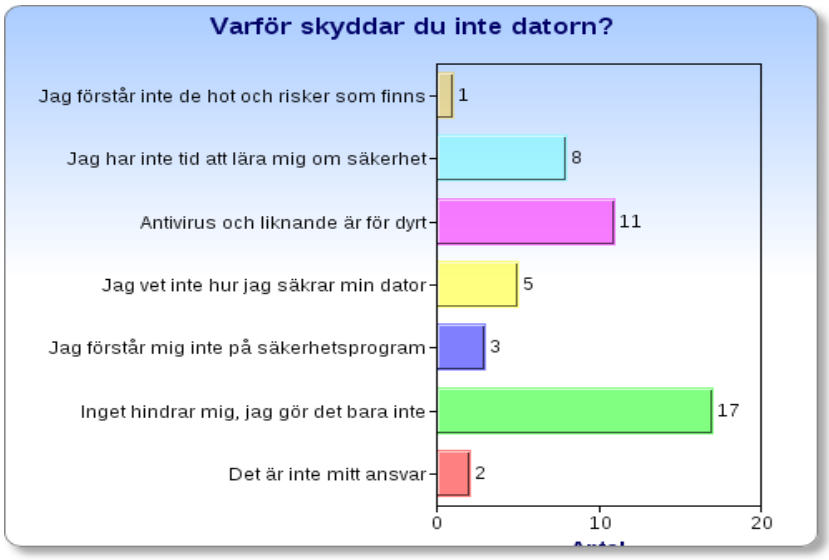
På frågan om vilka skydd som personerna hade på sin hemdator svarade 24 att de hade brandvägg, 34 svarade att de hade antivirus, 5 hade antispyware, 3 hade antispam och 4 personer visste inte. Tabell 8 presenterar resultatet.




*Tabell 8: Tabell över vilka skydd de tillfrågade hade på sin hemdator.*

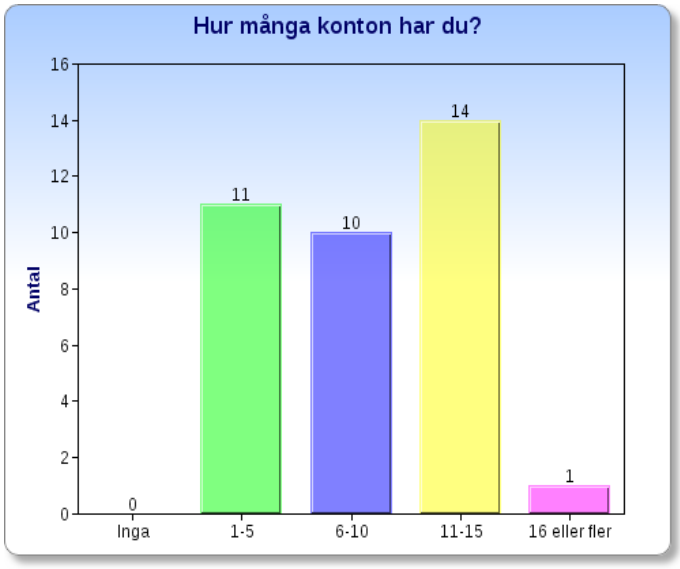
När frågan ställdes om personen tyckte att deras hemdator var säkrad mot Internetrelaterade hot och risker svarade 18 ja, 4 svarade nej och 16 visste inte.
På frågan om personen ansåg att det var viktigt att skydda sig mot de hot och risker som Internet medför svarade 34 personer ja, 0 personer nej och 4 personer visste inte.
Alla de 18 som svarade ja på frågan om de ansåg att deras hemdator var säkrad mot hot och risker hade både brandvägg och antivirus, även de som valt antispyware och antispam tillhörde gruppen som svarat ja.

Nästa fråga gällde varför man inte skyddar sin dator. På denna fråga fick personerna välja flera alternativ som de tyckte stämde in på dem, resultatet presenteras i tabell 9. De mest intressanta resultaten på denna fråga är att 8 personer ansåg att de inte hade tid, 11 tyckte att antivirusprogram och liknande var för dyrt och 17 personer lät helt enkelt bli att skydda sin dator.




*Tabell 9: Tabell över vilka orsaker som gjorde att personerna inte skyddar sin dator.*

På frågan om hur många konton personerna trodde att de hade på Internet svarade 11 personer att de hade 1-5 konton, 10 personer svarade 6-10, 14 personer svarade 11-15 och 1 person svarade att den hade 16 konton eller fler. Se tabell 10.




*Tabell 10: Tabell över hur många Internetkonton de tillfrågade hade.*

Fråga 17-21 i enkäten handlar om visualisering och den prototyp som presenterats. I avsnitten diskussion och slutsats kommer dessa svar att diskuteras tillsammans med vissa av de åsikter och funderingar som framkom i de kvalitativa intervjuerna.
När personerna fick frågan om de skulle tycka att det vore intressant att se resultatet om ett program ritade upp deras konton och kopplingar svarade 28 personer ja, 1 person nej och 9 personer hade ingen åsikt.
När enkäten sedan presenterat en pappersprototyp och en kort förklaring av det föreslagna programmet ställdes frågan om personerna förstod programmet och om de skulle kunna tänka sig att använda det. Det var endast 1 person som inte förstod programmet eller beskrivningen, 14 förstod programmet men tyckte det var ointressant eller irrelevant och 23 förstod programmet och kunde tänka sig att testa det. Vi valde att ha en följdfråga där vi undrade varför personer tyckte att programmet var ointressant eller irrelevant, detta för att kunna finna brister i prototypen och även för att förstå varför personerna svarat som de gjort. 3 svarade att de redan visste om de hot och risker som Internet medför, 5 personer ansåg att programmet verkade krångligt och 6 personer angav annan orsak.
På frågan om hur personerna skulle föredra att skaffa sig information om hot, risker och konton svarade 17 att de skulle vilja läsa sig till kunskapen själva, 16 svarade att de skulle föredra ett program likt prototypen och 5 hade ingen åsikt.
Av de 16 som svarade att de skulle använda sig av programmet hade 14 tidigare uttryckt att de hade liten eller ingen kunskap om de begrepp som det frågats om tidigare. Alla de som tidigare svarat att de hade medel eller god kunskap om phishing, tjojaner och spyware föredrog att läsa sig till kunskap om hot och risker.
Vi avslutade enkäten med att fråga om personernas medverkan i denna undersökning har fått dem att fundera på hur säker deras dator och deras konton är. 28 personer svarade ja, 9 nej och 1 person svarade att den inte hade någon åsikt.

# 7. Diskussion och slutsats

Detta avsnitt är uppdelat i fyra delar, vi kommer först att reflektera över vår egen undersökning och göra en värdering av vårt arbete. Vi kommer sedan att diskutera resultatet av vår undersökning för att sedan, i slutsats, besvara vår frågeställning. Uppsatsen avslutas med förslag till fortsatt forskning.

## 7.1. Reflektion

Vi kommer nu att reflektera över vår undersökning och göra en värdering av vårt arbete. Vi har valt att presentera de aspekter av undersökningen som har varit problematiska eller som gått extra bra.
Inledningsvis hade vi planerat att endast utforska människors kunskap och medvetenhet om Internetrelaterade hot och risker, men som vi beskrivit tidigare var den relaterade forskningen i ämnet fortfarande aktuell och utförlig. Vi valde då att utöka undersökningen med en del om visualisering och ett visualiseringsverktyg men att fortfarande behålla enkätundersökning som vårt datainsamlingsverktyg. Vi insåg också att om vi ska fråga om ett visualiseringsverktyg så krävs det en slags bild eller prototyp av det som ska utvärderas. Utvecklingen av ett program eller en prototyp är i högsta grad en iterativ process där tester och återkoppling är viktigt, detta gjorde att vi fick ta beslutet att också ha en mindre förundersökning där vi kunde få den återkoppling vi behövde, även om den bara gällde en grov skiss av ett program. Vi är av åsikten att det finns mycket bättre metoder än kvantitativ enkät om man faktiskt ska utveckla en It-artefakt, exempelvis ADR, action design research, men även kvalitativa intervjuer är att föredra.

Enkätundersökningen fyllde sitt syfte bättre när den användes för att undersöka kunskap och medvetenhet, de svarande tycktes förstå frågorna och nästan alla svarade på alla frågor.
När det kommer till frågornas utformning och de resultat vi fick anser vi att undersökningen gått bra, vilket validitet och reliabilitetsavsnitten visar. Det är ett fåtal frågor som kan ha formulerats bättre. Vid ett flertal tillfällen där alternativet annan orsak har använts har det senare visat sig att detta skapar frågetecken om varför personen svarat så och vi har endast kunna spekulera i det. Vi misstänker också att det finns ett mörkertal av personer som svarat att de inte vet något om exempelvis phishing och spyware även fast de egentligen gör det, det är de engelska termerna de inte har kommit i kontakt med tidigare. Detta baserar vi på att vi i förundersökningen fick förklara vissa hot och att intervjupersonerna då visste att dessa hot fanns, men de visste inte att det hette exempelvis phishing eller spyware.
Vår slutliga kommentar om denna undersökning är att den i allmänhet gått bra, den är valid och reliabel, vi har fått svar på vår frågeställning och vi fick in tillräckligt med data för att kunna diskutera resultatet. Vi valde kanske ett omständligt sätt att utföra utforskningen på, men i slutänden fick vi tillräckligt med material för att komma till en slutsats.

## 7.2. Diskussion

För att ta reda på hur man med hjälp av visualisering kan öka hemanvändares medvetenhet om Internetrelaterade hot och risker måste man också förstå användaren. Vi har med hjälp av vår enkät och våra intervjuer fått en bild av de olika användarnas kunskap och vanor när det gäller Internet, hot och risker. Detta för att kunna utforska vilken sorts användare som är intresserade av ett visualiseringsverktyg och hur detta verktyg ska utformas för att faktiskt öka medvetenheten.
Vår undersökning visar att intresse av datorer, Internet och informationssäkerhet är det som gör att en person kan och är mer medveten om Internetrelaterade hot och risker. Hur många år en person använt sig av Internet och vilket operativsystem som används hade enligt denna undersökning ingen inverkan på hur medveten och kunnig en person är. Resultatet visar också att det finns ett behov av att öka medvetenheten hos användare då många inte visste om deras dator var säker och vilka hot som finns.
En stor del av de som deltagit i denna undersökning har hemdatorer som används av flera personer, många av dessa är Windowsdatorer där användaren antingen loggar in, eller loggas in, automatiskt som administratör. En dator är inte säkrare än sin minst kunnige och medvetne användare. Att logga in som administratör ger användaren tillgång och möjligheten att ändra i exempelvis systemfiler och om man av misstag beviljar en installation av ett malware får detta tillgång till fler vitala filer än om man varit inloggad som användare. Många i undersökningsgruppen visste inte heller något eller hade bara hört talas om exempelvis phishing och spyware och loggade dessutom in som administratörer eller svarade att operativsystemet bara startade.
Många av de som deltog i undersökningen använder Internet till att shoppa, skicka och ta emot filer och till sociala medier, detta är platser och sätt där man komma i kontakt med ett antal hot och risker. Många av dessa personer har samtidigt ingen eller liten kunskap om exempelvis trojaner eller phishing, detta ökar dessa personers risk att bli lurade eller infekterade av malware. Slutligen anser många att deras dator är säker då de har antivirus och brandvägg installerat, vilket inte garanterar säkerhet.
Genom att ett visualiseringsverktyg visar kopplingarna mellan dator, e-post och konton på internet kan man visa för användarna att ett klick av misstag kan ge hackare tillgång till olika konton och i värsta fall hela datorn. Samtidigt bör verktyget informera om hur man kan skydda sig och beskriva specifika hot för kontot användaren är intresserad av, detta då undersökningen visar att många inte hört talas om eller förstår de risker som

användandet av Internet medför. Många av de som deltagit i undersökningen är också av uppfattningen att deras dator är säker för att de har antivirus och brandvägg, det bör därför förmedlas information om att så inte är fallet.
Nästan alla av de tillfrågade påstod sig tycka att det är viktigt att säkra sin dator och att de även skulle vilja lära sig mer om hot och risker, vilket tyder på en vilja hos personer att öka sin kunskap och medvetenhet. Detta samtidigt som 17 personer helt enkelt inte säkrade sin dator, utan motivation varför. Många tyckte också att antivirus och liknande var för dyrt eller att de inte hade tid att lära sig om säkerhet. Ett visualiseringsverktyg om konton, hot och risker bör därför utnyttja de ”väckarklockor” som de kvalitativa intervjuerna presenterade som resultat, detta för att väcka ett tidigt intresse hos användarna. På grund av att många av de som svarat på enkäten anser att de inte har tid att lära sig om hot och risker bör verktyget förmedla kort och tydlig information om säkerhet gällande konton och hur man skyddar sig, de borde också informeras om de gratisalternativ av, exempelvis antivirus, som finns när det gäller att skydda sig mot Internetrelaterade hot och risker.
Många av de som deltog i enkätundersökningen var av åsikten att de skulle tycka att det var intressant att se resultatet av att alla deras konton på Internet och de kopplingar de hade ritades upp av ett program. När personerna sedan blivit introducerade till en bild av en prototyp och en förklaring om hur programmet skulle fungera ansåg 23 personer att de skulle kunna tänka sig att testa ett sådant program. 5 personer ansåg att prototypen verkade krånglig. Detta resultat pekar på att ett visualiseringsverktyg är av intresse för många användare. Sista frågan som var av vikt för vår prototyp var hur personer skulle föredra att skaffa information om konton, dess kopplingar och Internetrelaterade hot och risker. Här svarade, som vi tidigare presenterat, 17 personer att de skulle föredra att läsa sig till informationen själva och 16 personer svarade att de skulle föredra ett program som liknade prototypen. Det visade sig att det var de personer som hade lägst kunskap om hot, risker och datorer som skulle föredra ett program som hjälpmedel för att lära sig. Om ett visualiseringsverktyg ska utvecklas är användarupplevelsen viktig då det ska utbilda människor, och vi har redan sett i enkäten att prototypen uppfattas som krånglig av vissa. De som svarat detta är också personer som i resten av enkäten visat på låg kunskap och medvetenhet om hot och risker. Därför är ett program som uppfattas som enkelt att eftersträva. Detta bekräftas också i förundersökningen där två av de intervjuade antydde att det, eftersom de visste väldigt lite om hot, risker och konton, var viktigt för dem att verktyget gjorde det stora jobbet i form av visualisering och kopplingar.
Den kvalitativa undersökningen ger oss belägg för att man bör utnyttja de ”väckarklockor” upptacktes under intervjuerna, detta för att intervjupersonernas intresse för programmet ökade drastiskt när de fick den informationen. Verktyget borde vara estetiskt tilltalande då det i första hand ska användas och vara intressant för de personer som har minst kunskap om informationssäkerhet och datorer, och det får då inte skrämma bort ovana datoranvändare.
När det kommer till användbarhetsmål är det självklart viktigt att man har alla dessa i åtanke när man utvecklar ett visualiseringsverktyg. Men då många användare har liten kunskap om hot, risker och datorer anser vi att det viktigaste, förutom att det är effektivt, är att det ska vara lätt att lära sig, ha en bra förmåga att hjälpa användaren att utföra det den vill och att det ska vara säkert.

## 7.3. Slutsats

**Hur bör ett visualiseringsverktyg som ska öka hemanvändares kunskap och medvetenhet om Internetrelaterade hot och risker utformas?**
Vår undersökning visar på att man genom att utnyttja de ”väckarklockor” som nämnts i tidigare avsnitt kan väcka ett intresse hos användare för att vilja lära sig mer om informationssäkerhet, därför är det viktigt att ett visualiseringsverktyg tidigt presenterar hot och risker som användaren kan relatera till. Genom att sedan visualisera kopplingar mellan dator, e-post och konton på internet kan man visa för användarna hur sårbara deras datorer och konton är eller kan vara. Genom att göra denna information tydlig i ett tidigt skede kan man också väcka intresset hos de som anser att de inte har tid att lära sig om hot och risker.
Att verktyget samtidigt informerar om hur man kan skydda sig mot hot och risker, och även beskriver specifika hot gällande konton och hemsidor användaren använder sig av skapar det ett intresse och en vilja att lära sig mer. Undersökningen visar också att man bör utnyttja prototypen för att upplysa användare om att brandvägg och antivirus inte garanterar en säker dator och man bör också föreslå antivirusprogram och andra skydd som är gratis.
Användarupplevelsen är viktig och ett program som uppfattas som enkelt att använda är att eftersträva, det bör också vara upplysande och intressant. Extra viktiga användbarhetsmål då många användare har liten kunskap om hot, risker och datorer är att verktyget är effektivt, lätt att lära sig, och det ska ha en bra förmåga att hjälpa användaren att utföra det den vill, det bör också vara säkert att använda.

## 7.4. Förslag till fortsatt forskning

Frågan om hur man ska öka människors medvetenhet om Internetrelaterade hot och risker är i högsta grad fortfarande aktuell, vi föreslår deärför i första hand att man utforskar fler sätt till hur denna medvetenhet och kunskap kan höjas.
Ett annat förslag är att forska kring de idéer som både Furnell m.fl. (2007) och Kritzinger m.fl. (2010) har om att man mer eller mindre ska tvinga människor att bli medvetna. Hur skulle sådana regler och restriktioner påverka hemanvändarna och och vad är deras åsikt i diskussionen?
Även en vidareutveckling av den protyp vi beskrivit i denna uppsats skulle vara intressant att utforska. Hur kan man göra den mer inbjudande och hur kan man få den att bli intressant även för kunniga och medvetna människor? Prototypen skulle också kunna ligga till grund för en vidareutveckling där programmet faktiskt genomför en riskanalys genom att undersöka datorn, konton och personers kunskap.

# 8. Referenser

Davidson, P. Patel, R. Forskningsmetodikens grunder - att planera, genomföra och rapportera en undersökning. Fjärde upplagan. Studentlitteratur, 2011

Furnell, S. Bryant, P. Phippen, D. Assessing the security perceptions of personal Internet users. Computers & Security 2007;26:410-7.

Furnell, S. Tsaganidi, V. Phippen, A. Security beliefs and barriers for novice Internet users. Computers & Security 2008;27:235-40.

Kim, W. Ok-Ran, J. Kim, C. So, J. The dark side of the Internet: Attacks, costs and responses. Information Systems 2011;36:675-705.

Kritzinger, E. von Solms, S.H. Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security 2010;29:840-47.

Löwgren, J. Stolterman, E. Design av informationsteknik, Studentlitteratur, 2004.

Sharp, H. Rogers, Y. Preece, J. Interaction Design: Beyond Human-Computer Interaction. Andra upplagan. Hoboken, NJ: John Wiley & Sons, 2007.

Withall, M. Phillips, I. Parish, D. Network visualisation: a review. IET Communications 2007;1:365-72.

# Bilaga – missiv och enkät

## Missiv

Vi heter Magnus och Aram och läser vårt tredje år på Göteborgs Universitet, systemvetenskapligt program. Som avslutning på läsåret skriver man en uppsats där man forskar om ett visst fenomen. Vi skulle bli väldigt glada om ni tog er tid att fylla i denna enkät för att hjälpa oss att samla in den information vi behöver för att kunna slutföra vårt arbete.

Denna undersökning handlar till stor del om Internetrelaterade hot och risker, men låt inte detta avskräcka er. Det är viktigt för undersökningen att personer med olika erfarenhet, kön, ålder och utbildning svarar på den. Denna undersökning gäller inte de datorer ni använder på ert arbete, utan datorer ni har i hemmet och era privata bärbara datorer. Denna undersökning har alltså ingen koppling till er arbetsplats och inga av era chefer eller medarbetare kommer att kunna ta del av hur just ni har svarat.

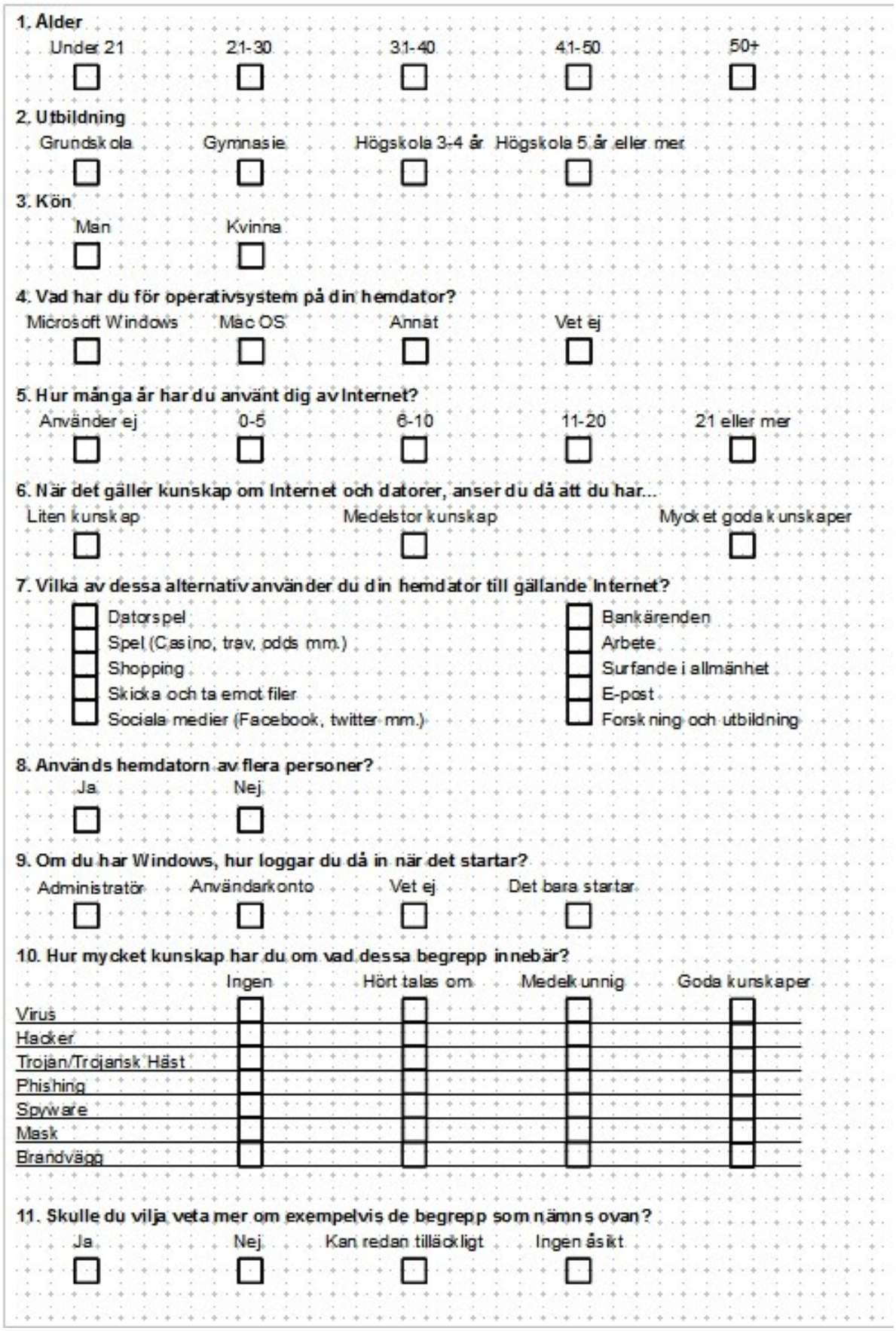
Vi kommer inte att jämföra åldersgrupper, utbildning eller kön i själva uppsatsen, dessa frågor är med för att se till att alla som svarar inte är 20 år, bara män eller liknande, då detta skulle resultera i ett missvisande resultat i uppsatsen.

Enkäten är helt anonym och det finns inga ”rätta” svar, så var ärliga. Om inget av svarsalternativen passar eller om du inte vill svara på frågan är det fritt att lämna den obesvarad.

Tack på förhand

/Magnus och Aram

# Enkät



1. Ålder

Under 21 ☐ 21-30 ☐ 31-40 ☐ 41-50 ☐ 50+ ☐

2. Utbildning

Grundskola ☐ Gymnasie ☐ Högskola 3-4 år ☐ Högskola 5 år eller mer ☐

3. Kön

Man ☐ Kvinna ☐

4. Vad har du för operativsystem på din hemdator?

Microsoft Windows ☐ Mac OS ☐ Annat ☐ Vet ej ☐

5. Hur många år har du använt dig av Internet?

Använder ej ☐ 0-5 ☐ 6-10 ☐ 11-20 ☐ 21 eller mer ☐

6. När det gäller kunskap om Internet och datorer, anser du då att du har...

Liten kunskap ☐ Medelstor kunskap ☐ Mycket goda kunskaper ☐

7. Vilka av dessa alternativ använder du din hemdator till gällande Internet?

☐ Datorspel
☐ Spel (Casino, trav, odds mm.)
☐ Shopping
☐ Skicka och ta emot filer
☐ Sociala medier (Facebook, twitter mm.)
☐ Bankärenden
☐ Arbete
☐ Surfande i allmänhet
☐ E-post
☐ Forskning och utbildning

8. Används hemdatorn av flera personer?

Ja ☐ Nej ☐

9. Om du har Windows, hur loggar du då in när det startar?

Administratör ☐ Användarkonto ☐ Vet ej ☐ Det bara startar ☐

10. Hur mycket kunskap har du om vad dessa begrepp innebär?

| | Ingen | Hört talas om | Medelkunnig | Goda kunskaper |
|---|---|---|---|---|
| Virus | ☐ | ☐ | ☐ | ☐ |
| Hacker | ☐ | ☐ | ☐ | ☐ |
| Trojan/Trojansk Häst | ☐ | ☐ | ☐ | ☐ |
| Phishing | ☐ | ☐ | ☐ | ☐ |
| Spyware | ☐ | ☐ | ☐ | ☐ |
| Mask | ☐ | ☐ | ☐ | ☐ |
| Brandvägg | ☐ | ☐ | ☐ | ☐ |

11. Skulle du vilja veta mer om exempelvis de begrepp som nämns ovan?

Ja ☐ Nej ☐ Kan redan tillräckligt ☐ Ingen åsikt ☐

12. Anser du själv att din hemdator är säkrad mot Internetrelaterade hot och risker?

Ja ☐ Nej ☐ Vet inte ☐

13. Vilka av dessa skydd har du i datorn?

Brandvägg ☐ Antivirus ☐ Antispyware ☐ Antispam ☐ Vet ej ☐

14. Tycker du det är viktigt att skydda sin hemdator mot de risker och hot som Internet medför?

Ja ☐ Nej ☐ Vet inte ☐

15. Om du är av åsikten att du troligtvis skulle kunna skydda din dator mer men ändå inte gör det, varför är det så? Du kan välja flera alternativ

- ☐ Jag förstår de hot och risker som Internet medför och lägger ner tid på att säkra min dator.
- ☐ Det är inte mitt ansvar att säkra datorn.
- ☐ Inget hindrar mig, jag gör det bara inte.
- ☐ Jag tycker inte att det är viktigt.
- ☐ Jag förstår mig inte på säkerhetsprogram (antivirus och liknande).
- ☐ Jag vet inte hur jag säkrar min dator.
- ☐ Antivirusprogram och liknande är för dyra.
- ☐ Jag har inte tid att lära mig om- och hantera min dators säkerhet.
- ☐ Jag förstår inte de hot och risker som finns.
- ☐ Innan denna undersökning visste jag inte att det fanns några hot eller risker.

16. På Internet skapar man ofta olika konton med användarnamn och lösenord, exempelvis Webmail, Facebook, forum och shoppingsidor. Vet du hur många olika konton du har?

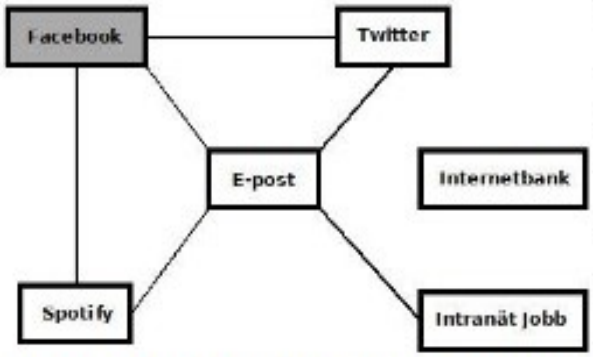
Inga ☐ 1-5 ☐ 6-10 ☐ 11-15 ☐ 15+ ☐

**Information:**

Ofta loggar man in på konton med sin e-postadress och ett lösenord, många personer använder samma lösenord på flera olika platser. Detta innebär att om någon får tag på ett sådant lösenord så kan de genom att testa sig fram ta över alla konton med samma lösenord.

Dina konton är i allmänhet kopplade till din e-post, och med hjälp av din e-post kan du ofta återställa lösenord och användarnamn du glömt. Detta innebär att om någon tar över din e-post så är chansen stor att de kan ta sig in och/eller ta över *alla* konton som är kopplade till e-posten.

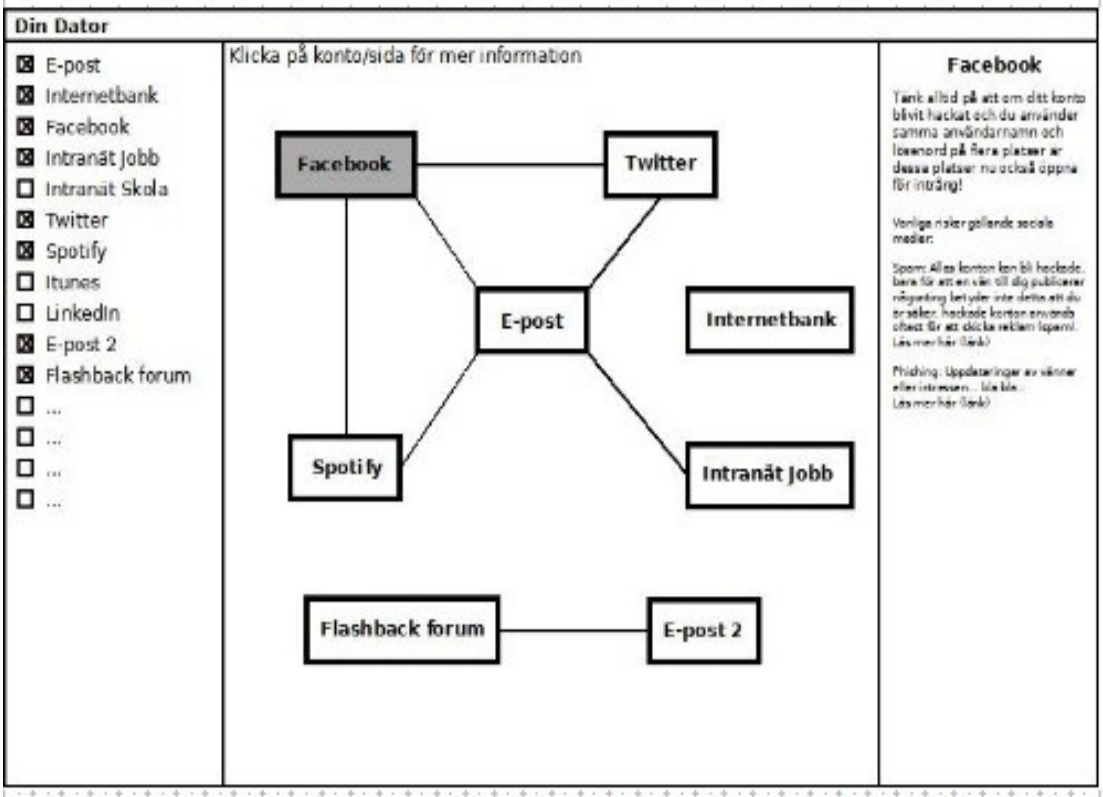
Om man ritade sina konton och dess kopplingar till varandra skulle resultatet kunna se ut såhär:




17. Om ett program ritade upp alla dina egna konton och dess kopplingar på samma sätt som ovan, skulle du då tycka att det vore intressant att se resultatet?

Ja ☐ Nej ☐ Ingen åsikt ☐

**Titta på denna bild:**




Denna bild föreställer ett program som till vänster låter dig själv välja de konton du har. Du får då upp dessa konton och dess kopplingar i mitten, där du då kan klicka på dem för att få mer information om vad du borde tänka på när du besöker sidan. Där får du även kortfattad information om vanliga hot, till exempel spam, phishing och hacking.

**18. Gällande bilden och beskrivningen ovan; vilket av dessa påståenden håller du med om?**

- ☐ Jag förstår inte bilden och/eller beskrivningen.
- ☐ Jag förstår bilden och beskrivningen men tycker att det är ointressant/irrelevant.
- ☐ Jag förstår bilden och beskrivningen, och skulle kunna tänka mig att testa programmet.

**19. Om du valt att programmet är ointressant eller irrelevant, varför är det så?**

- ☐ Dålig design.
- ☐ Jag är redan medveten om de hot och risker som finns.
- ☐ Jag tycker inte att säkerhet på min hemdator är viktigt.
- ☐ Det verkar krångligt.
- ☐ Annan orsak.

**20. Om du var tvungen att lära dig om konton och säkerhet, skulle du då föredra att läsa om detta på en hemsida eller skulle du hellre göra det mer personligt och använda ett program som detta?**

| Läsa på hemsida | Detta program | Annat sätt | Ingen åsikt |
|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ |

**21. Sista frågan. Har denna enkät fått dig att fundera över hur säker din hemdator och dina konton på Internet är?**

| Ja | Nej | Ingen åsikt |
|---|---|---|
| ☐ | ☐ | ☐ |

**Tack för din medverkan!**