



2005-10-18
Lund

Institutionen för informatik

Internetanvändning och säkerhet hos privatpersoner

Kandidatuppsats, 10 poäng, inom Systemvetenskapliga programmet

Framlagd: 18 oktober, 2005

Författare:

Jesper Rodriguez 710201
Linus Pålstorp 830728

Handledare:

Anders Svensson

Internetanvändning och säkerhet hos privatpersoner

Kandidatuppsats framlagd: 18 oktober, 2005
Författare: Jesper Rodriguez och Linus Pålhlstorp
Omfång: 59 sidor
Handledare: Anders Svensson

Abstrakt

Internetanvändandet i Sverige har ökat under flera år och det finns tendenser på att det fortsätter att öka. Det ökande användandet medför inte bara positiva aspekter utan även negativa aspekter som olika Internetrelaterade hot och risker som kan drabba användare. Syftet med denna uppsats var att ta reda på om Internetanvändningen och dess aktiviteter och tjänster fortsätter att öka. Ytterligare en anledning var att undersöka om kunskapen och medvetenheten om Internetrelaterade hot och risker har ökat hos Internetanvändare samt hur de skyddar sin dator mot de olika hoten och riskerna. För att styrka och få bättre relevans på uppsatsen innehåller teorikapitlet bland annat korta beskrivningar om de vanligaste begreppen inom Internetrelaterade hot, risker och säkerhetsskydd samt statistik om hur Internetanvändandet har sett ut de senaste åren. Genom en kvantitativ enkätundersökning, som gjordes på ett begränsat urval, fick vi fram data om våra respondenters Internetanvändning som sedan jämfördes mot tidigare undersökningar. Detta resulterade i tydliga tendenser på att Internetanvändandet, medvetenheten om Internetrelaterade hot och risker samt hur man skyddar sig mot de olika hoten och riskerna har ökat.

Nyckelord: Internetanvändning, aktiviteter, tjänster, hot, risker, säkerhetsskydd

Innehållsförteckning

1 Inledning.....	4
1.1 Bakgrund	4
1.2 Vad är vår problemställning?	4
1.3 Varför denna uppsats?	5
1.4 Avgränsning	6
1.5 Disposition	6
2 Metod	7
2.1 Kvantitativ – kvalitativ	7
2.2 Primär- och sekundärkällor	7
2.3 Källkritik	7
2.4 Reliabilitet och Validitet	8
2.4.1 Reliabilitet	8
2.4.2 Validitet	8
2.5 Urval.....	8
2.6 Empirisk undersökning	9
2.6.1 Enkätutformningen.....	9
2.6.2 Enkätfrågorna	10
3 Tillgång, användning och säkerhetsproblem av Internetuppkopplade hemdatorer.....	12
3.1 Tillgång till datorer i hemmen.....	12
3.2 Tillgång till Internet i hemmen.....	13
3.3 Användning av Internet i hemmen	15
3.4 Säkerhetsproblem vid användning av Internet	16
4 Säkerhetsrisker	17
4.1 Skadlig kod.....	17
4.1.1 Datavirus	19
4.1.2 Maskar	19
4.1.3 Trojan/Trojansk häst	19
4.1.4 Bakdörr (Trapdoor)	20
4.2 Portskanning.....	20
4.3 Spam.....	20
4.4 Spionprogram (Spyware) och liknande.....	21
4.5 Hacker och cracker.....	21
4.5.1 Hacker	21
4.5.2 Cracker	22
5 Skydd.....	23
5.1 Brandvägg	23
5.2 Antivirusprogram	23
5.3 Användarpolicy	24
5.4 Krypteringsprogram	24
5.5 Filtreringsprogram som hindrar besök på osäkra sidor	25
5.6 Säkerhetsuppdateringar	25
6 Enkätanalys	26
6.1 Utförande.....	26
6.2 Analys av enkätfrågorna.....	26
7. Resultat - diskussion.....	32
7.1 Ökad uppkopplingstid	32
7.2 Ökad användning av fast anslutning	35
7.3 Aktiviteter och tjänster på Internet.....	37

7.4 Säkerhetsmedvetande hos privatpersoner	40
7.5 Säkerhetsåtgärder hos privatpersoner.....	44
8 Slutsats	46
9 Vidare forskning.....	47
10 Källförteckning.....	48
11 Bilagor.....	50
11.1 Enkät.....	50
11.2 Enkättemanställning.....	53

1 Inledning

1.1 Bakgrund

Genom den ökande takten av beroendet av information, blir folk mer och mer beroende av att ha datorer i hemmet. Det räcker inte med att bara ha en dator, den måste numera vara uppkopplad mot Internet. Till en början med var inte behovet speciellt stort och det räckte med att använda sig av kortare Internet sessioner. Mängden data man bytte var inte heller speciellt omfattande. Detta håller på att ändras, eftersom man gör allt mer med sin hemdator, allt från att läsa tidningen online till att spela onlinespel. För att underlätta användningen av Internet från hemmet så väljer fler och fler olika typer av bredbandslösningar, vilket innebär att man är uppkopplad under längre sessioner. Längre uppkopplingstid medför att man finns på Internet under längre tid och därmed är man mottaglig för andra personer att hitta din dator på Internet.

1.2 Vad är vår problemställning?

Vår problemställning innebär att vi vill undersöka eventuella tendensskillnader när det gäller hur Internetanvändandet och medvetenheten om Internetrelaterade skydd, hot och risker ser ut hos privatpersoner. För att kunna besvara vår problemställning behöver vi ett antal frågeställningar. Dessa frågeställningar tog vi fram genom att vi byggde upp en hypotesdialog om hur vi trodde det kunde se ut.

- *Hur ofta använder ni Internet i hemmet?*
- *Tja, det har blivit mer och mer nu sedan vi har skaffat bredband. Det ångrar jag mig inte eftersom våra Internetkostnader har sjunkit drastiskt. Jag själv använder Internet för att läsa mina e-mail samt att läsa de senaste nyheterna och sporthändelserna. Detta brukar ta ungefär 30-60 minuter per dag.*
- *Är det någon annan i familjen som brukar koppla upp sig?*
- *Frun, brukar också vara uppkopplad 30-60 minuter varje dag. Det är hon som har hand om vår ekonomi och betalar räkningarna online. Sen har vi våra barn Lisa 15 och Kalle 18, de är uppkopplade så ofta som möjligt. Uppskattningsvis står de kanske för 4-6 timmar per dag.*
- *Nu eftersom ni är uppkopplade ungefär 5-6 timmar per dag, har ni då tänkt på någon typ av säkerhet?*
- *Tänkt på det, men är inte så hemma på datorer. Mina kunskaper om datorer går så långt som att jag kan starta och stänga av en dator. Samt att jag kan göra de flest vanliga sakerna på den, såsom att skriva, surfa och läsa/skicka e-mail. Min son installerade någonting, ett antivirusprogram och en brandvägg tror jag det var. Antivirusprogrammet var enkelt, eftersom det skötte sig själv, men brandväggen var en annan historia, det slutade med att jag bad honom ta bort det, för saker och ting slutade fungera samt att det kom konstiga meddelande som jag inte visste vad jag skulle svara på.*

Utifrån hypotesdialogen plockade vi ut följande fem frågeställningar som kunde ge svar på vår problemställning.

- **Ökad uppkopplingstid**
En ökad uppkopplingstid mot Internet kan medföra att en användare utsätter sig för större risk att råka ut för olika typer av Internetrelaterade hot och risker. Därför vill vi undersöka om nyttjandet av nätet har ökat.
- **Ökad användning av någon typ av fast Internetanslutning**
Personer som har någon typ av fast Internetanslutning¹, tenderar att vara uppkopplad mot Internet under längre perioder än personer som använder sig av någon typ av uppringd Internetförbindelse². Ökad uppkoppling medför ökad risk för Internetrelaterade hot och risker. Därför vill vi undersöka om fasta anslutningar hos privatpersoner har ökat.
- **Aktiviteter och tjänster på Internet**
Beroende på vilka Internetrelaterade aktiviteter och tjänster en användare utför kan han eller hon utsättas för olika typer av hot och risker. Därför vill vi undersöka vad en privatperson utför på Internet.
- **Säkerhetsmedvetandet hos privatpersoner**
Det finns en mängd hot och risker som är kopplat med Internetanvändning. Därför vill vi undersöka hur säkerhetsmedvetna privatpersonerna är.
- **Säkerhetsåtgärder hos privatpersoner**
Det finns en mängd säkerhetsåtgärder för att skydda sig mot Internetrelaterade hot och risker. Därför vill vi undersöka vad eller vilka säkerhetsåtgärder en privatperson gör för att skydda sig mot dessa.

1.3 Varför denna uppsats?

Vårt syfte med denna uppsats är att ta reda på privatpersoners Internetanvändning och deras medvetenhet om Internetrelaterade skydd, hot och risker. Detta ska vi göra med hjälp av litteraturstudier och en kvantitativ empirisk frågeundersökning i form av en enkätundersökning. Utifrån denna enkätundersökning kommer vi att analysera och jämföra svaren mot tidigare undersökningar, för att sedan påvisa eventuella tendensskillnader och varför vi har fått de svar vi har fått från vår undersökning.

¹ Fast Internetanslutning – Vår definition: Kostnaden för Internet är inte beroende på hur mycket man nyttjar det. Till dessa räknar vi bl.a.: Fast (nätverk), ADSL, DSL, Kabelmodem.

² Uppringd Internetförbindelse – Vår definition: En Internetanslutning som man betalar för den tid man nyttjar Internet. Till dessa räknar vi bland annat: Modem (Telefon), ISDN, Mobil.

1.4 Avgränsning

I denna uppsats kommer vi att avgränsa oss till att titta på privatpersoners Internetanvändning och deras medvetenhet om säkerhet, hot och risker relaterat till Internet. Vi kommer att förklara på ett enkelt sätt en del hot och säkerhetstermer i kapitel 4 och 5, som är kopplat till de frågor vi har på enkäten. Vi kommer inte att gå djupt in på något av de tekniska områden som kan tänka sig komma upp i uppsatsen, för det är inte vad som är syftet med denna uppsats. Tekniska termer som ligger utanför vårt område, det vill säga termer som inte finns med på enkäten kommer inte tas upp.

Vidare kommer vi att avgränsa vår population geografiskt, de personer som kommer att svara på vår enkät, till enbart personer som bor i Sverige.

1.5 Disposition

Abstrakt

En sammanfattning av hela uppsatsen

Inledning (kap 1)

En kortare bakgrund om varför vi har valt att göra just denna undersökning. Här finns även uppsatsens syfte, vår problemställning och frågeställningar.

Metod (kap 2)

Förklarar vilken typ av metod vi använt oss av samt kortare teori om källor, urval och tillförlitlighet när det gäller reliabilitet och validitet.

Teori (kap 3-5)

Bakgrundsinformation och statistik om privatpersoners Internetanvändning har sett ut de senaste åren samt kortare ämnesrelaterad teori om Internetrelaterade hot, risker och skydd.

Enkätanalys (kap 6)

Redogörelse om hur vår enkätundersökning resulterade samt sammanställningar av våra enkätsvar.

Resultat-diskussion (kap 7)

Här diskuteras våra frågeställningar genom att jämföra vår undersökning mot tidigare undersökningar. Diskussionen leder sen till att vi kan svara på våra frågeställningar.

Slutsats (kap 8)

Med hjälp av det vi kom fram till i kapitlet *Resultat-diskussion*, där vi svarade på våra frågeställningar, kan vi besvara vår problemställning som i sin tur svarar på vårt syfte.

2 Metod

Vi kommer att använda oss av litteraturstudier, för att inhämta information angående vårt arbete. Vi kommer även att göra en empirisk undersökning som kommer att innehålla en enkätundersökning. Den empiriska undersökningen kommer sedan att sammanställas och analyseras enligt våra frågeställningar för att sedan jämföras mot tidigare liknande undersökningar.

2.1 Kvantitativ – kvalitativ

När man behandlar en frågeställning finns det två olika större metoder att genomföra sin forskning på, nämligen att antingen göra den kvantitativt eller kvalitativt. Det går även att blanda de olika sätten när man utför sin forskning. Skillnaden mellan dem i stora drag kan vid en första anblick vara att en kvantitativ forskare i första hand bara mäter olika företeelser medan en kvalitativ forskare inte gör det. Men det finns forskare och författare som menar att olikheterna går djupare än huruvida man använder sig av kvantifiering eller inte. [Bryman, 2004]

Beroende på vår problemställning och våra frågeställningar har vi valt att utföra en kvantitativ undersökning. Det beror framförallt på att vi vill få fram "hur det ser ut" i samhället och hitta samband och andra faktorer som kan påverka resultatet.

2.2 Primär- och sekundärkällor

I vår kvantitativa undersökning utgår vi från en egen skapad enkät som vi använder som primärkälla. Med primärkälla (förstahandskälla) menas att det är en ursprungligkälla som inte har publicerats tidigare. För att styrka informationen om den data som vi får ut från vår primärkälla använder vi oss av sekundärkällor (andrahandskällor) som består av bland annat böcker, webbdokument, andras rapporter och uppsatser. Sekundärkällor är alltså sådana källor som publicerats tidigare (gått i flera led). [Anderberg, 2004]

2.3 Källkritik

När man ska bedöma fakta från en källa gäller det att man ser på den med kritiska ögon och ställer frågor som *När och Varför tillkom källan? Vilket syfte hade upphovspersonen med det han/hon skrev? Vem/vilka har skrivit informationen?* etc. [Patel & Davidsson, 1994]

Tittar man på de källor vi använde oss av i denna uppsats så var vår primärkälla, som bestod av en enkät, av väsentlig betydelse. I och med att vi själva tillverkade enkäten så var det svårt för oss att se den som en kritisk källa. Däremot var vi tvungna att ha stor tillförlit till våra respondenter att de var ärliga i sina svar.

Ytterligare använde vi oss av litterära böcker, rapporter och Internetsidor som sekundärkällor i uppsatsen. Det är framförallt sekundärkällorna man måste granska med ett kritiskt öga. Generellt sett så är fakta från litterära böcker och rapporter, speciellt vetenskapliga, trovärdiga men däremot är det mer osäkert med Internetsidor. När det gäller Internetsidor använde vi oss

av, i så stor mån som möjligt, sidor från myndigheter eller stora samarbetspartner till dem och från kända företag och verksamheter. Man kan även vara källkritisk mot dessa sidor men vi ansåg att informationen på dessa sidor var trovärdiga eftersom de stämde överens med vår erfarenhet och tidigare kunskaper om ämnet. Därför kommer vi att använda oss av följande tre tidigare undersökningar när vi kommer att jämföra våra resultat: *Privatpersoners användning av datorer och Internet 2003* (SCB, 2004), *Privatpersoners användning av datorer och Internet 2004* (SCB, 2004) och kandidatuppsatsen *Datasäkerheten i hemdatorerna* (Hagman & Meltzer, 2002)

2.4 Reliabilitet och Validitet

För att bedömningen av en samhällsvetenskaplig undersökning ska vara så relevant som möjligt gäller det att de som utför undersökningen uppfyller vissa kriterier. Två av dessa kriterier är *reliabilitet* och *validitet*. [Bryman, 2004]

2.4.1 Reliabilitet

Begreppet reliabilitet eller tillförlitlighet innebär att man bland annat mäter hur tillförlitligt en undersökning är. När utgångspunkten för en undersökning är gjord med hjälp av en enkät, så som vi har gjort, är det svårt att kontrollera hur tillförlitlig den är innan man har fått in resultatet på den. För att förebygga och försöka få bättre tillförlitlighet på sin enkät bör man försöka försäkra sig om att respondenten som ska svara har uppfattat enkäten som forskarna tänkt sig. Därför lät vi testpersoner titta igenom vår enkät för att ge synpunkter på utformningen av den. [Patel & Davidsson, 1994]

2.4.2 Validitet

Med validitet menas att man verkligen mäter det ”man avser att undersöka”. Det finns olika sätt att mäta validitet, till exempel när man utformar en enkät gäller det att den får en så bra *inhållsvaliditet* som det bara går. Bra *inhållsvaliditet* åstadkommer genom att det utförs en logisk analys av innehållet i ens instrument. Problemet är om forskarna själva skapat sitt instrument så är det lätt att tro att *inhållsvaliditeten* är hög och därmed ser man inte sina egna misstag. [ibid]

För att förbättra *inhållsvaliditeten* så har vi låtit testpersoner, som är utomstående från forskningen, svara på enkäten så vi kunde analysera svaren och se om svaren på frågorna verkligen mätte det som vi tänkt oss.

2.5 Urval

Vi hade tänkt använda oss av stickprovsurval till vår enkätundersökning. Med stickprovsurval menas att forskaren väljer ut intervjupersoner eller enkätpersoner slumpvist, utan någon hänsyn till ålder, kön eller utbildning för att öka både reliabiliteten och validiteten [Bryman, 2004].

Eftersom vår stickprovsundersökning fallerade, var vi tvungna att göra en ny undersökning. Vi valde då att göra en bekvämlighetsurvalsundersökning. Med en bekvämlighetsurvalsundersökning menas att forskaren väljer de personer som finns för stunden tillgängliga [ibid]. Därför valde vi vår bekantskapskrets samt deras vänner (se mer om detta i kap 6).

2.6 Empirisk undersökning

Vår empiriska undersökning består av en kvantitativ enkätundersökning. Vi har valt att göra den kvantitativ på grund av att vi vill få in så mycket material som möjligt från de olika målgrupperna. Detta för att sedan kunna göra en så bra analys som möjligt på hur säkerheten mot Internetrelaterade hot och risker ser ut hos allmänheten.

Varför vi har valt en enkätundersökning är på grund av vi är intresserade av respondenternas åsikter/attityder, vilket vi kan lättast styra deras åsikter med hjälp av konstruerade svar. Detta leder till att vi kan göra en mer noggrann analys eftersom svaren de har gett är mer strukturerade till det vi är intresserade av. [Andersson, 2001]

Att insamla information med hjälp av enkätundersökningar medför både fördelar och nackdelar. Detta beror på vilken typ av undersökning man är intresserad av att göra samt vad undersökningen skall leda till. Efter att ha övervägt fördelar mot nackdelar med enkätundersökningar i litteraturen av Bryman och Andersson, styrker detta ytterligare att en enkätundersökning var det rätta instrumentet för denna typ av undersökning.

2.6.1 Enkätutformningen

När vi utformande enkäten var det självklart väldigt viktigt att vi verkligen fick de svar som svarade på våra frågeställningar. Förutom att frågeställningarna blev besvarade var det viktigt att få själva formgivningen av enkäten så tilltalande som möjligt för att få folk att fylla i den.

Det finns en hel del tricks som används för att inte avskräcka respondenten från att fylla i enkäten. En enkät som är kort och tunn har större chans att folk besvarar än en enkät som ser stor och tjock ut. Det är oftast rekommenderat om man vill ha sin enkät att se mindre ut än vad den verkligen är, att man minskar typsnitt, radavstånd och marginaler. Men detta kan dock få den motsatta effekten, genom att respondenten upplever enkäten som arbetsam att besvara och det kvittar hur liten och tunn den är. Man får gärna göra dessa tricks för att göra sin enkät mindre i utseende, men det är mycket viktigt att man inte får enkäten för tät, för då kommer det att upplevas som rörig och överfull. [Bryman, 2004]

Med formgivningstricken i minnet försökte vi minska de tre sidorna som enkäten innehöll. Vi testade att ha vår presentation på en helt egen sida, för att inte denna skulle upplevas som en del av själva enkäten. Efter det började vi formatera textstorlekar, marginaler och tätheten mellan frågorna. Resultatet blev att vi inte kunde komma ner på två sidor (tre sidor med vår presentation) utan att det blev för tätt och rörigt. Så vi bestämde att vi inte behövde göra någon formatering av själva layouten av enkäten och att tre sidor inte var så mycket, med tanke på att den var någorlunda luftig mellan de olika frågorna. En sak som vi kunde ha gjort var att trycka enkäten som dubbelsidig, men detta föll på att vi inte kunde få kopieringsmaskinen till att göra detta samt att en dubbelsidig enkät kan också leda till att folk glömmer att besvara frågorna som finns på baksidan av enkäten.

Utöver själva formgivningen av enkätlayouten så är det själva formgivningen av frågorna som måste göras på ett bra och ett så enkelt sätt för respondenten att svara på.

Det är viktigt att man ger tydliga instruktioner om hur svarandet skall gå till när man har slutna frågor. I många fall kan man inte täcka in alla de olika tänkbara svarsalternativ, då är det bra att ha ett alternativ som heter ”annat” som respondenten själv kan skriva in sitt svar på. En del fall så kan det vara oklart hur många alternativ respondenten skall fylla i, skall han eller hon fylla i endast ett alternativ eller flera [Bryman, 2004]. Just denna problematik har vi löst efter web praxis, fyrkantstrutor anger ett eller flera alternativ kan kryssas i medan cirklar anger att endast ett alternativ får kryssas i. Självklart så har vi instruktioner om detta på själva enkäten om vad kryss -fyrkanterna och -cirklarna betyder.

Vi har även varit noga med att hålla ihop frågorna med svarsalternativen och separerat frågorna med dess svarsalternativ med gott om tomrum för att respondenten lätt skall se vilka svar och frågor som hör ihop. [Bryman, 2004]

2.6.2 Enkätfrågorna

Vi startar enkäten med tre stycken personliga faktafrågor (**Fråga 1**, **Fråga 2** och **Fråga 3**). [Bryman, 2004]. Dessa frågor är såkallat uppdelningsfaktorer (kön, ålder och utbildning). Vi behöver dela in enkätsvaren enligt dessa uppdelningsfaktorer eftersom dessa kan påverka våra frågeställningar. Åldersindelningen i fråga 2, är direkt taget från SCB för att underlätta jämförelser mot deras tidigare undersökningar.

Fråga 4 är en fråga som tar reda på vilka som har eller inte har tillgång till en hemdator med Internetuppkoppling. Om enkätpersonen svarar nej eller vet ej, då behöver han/hon inte fortsätta att svara på efterföljande frågor. Det är endast de personer som har en hemdator med Internetuppkoppling som vi är intresserade av att få ytterliggare svar från.

Fråga 5 är konstruerad på det sättet att vi frågar efter hur de betalar för Internet, eftersom kostnader nästan alltid styr hur mycket man nyttjar Internet. Desto mer man nyttjar Internet desto mer mottaglig är man mot olika typer av Internetrelaterade hot och risker. Vidare skall denna fråga ge en del av svaret på vår frågeställning: ”Ökad användning av någon typ av fast Internetanslutning” (se kap 1.2).

Fråga 6. Genom att fråga enkätpersonerna om vilken typ av Internetuppkoppling de har i hemmet, kan vi ta reda på vilka av dem som har fast uppkoppling eller en uppringd förbindelse. Denna fråga är en del av vår problemställning: ”Ökad användning av någon typ av fast Internetanslutning” (se kap 1.2).

Fråga 7 frågar efter vilken är den främsta orsaken till valet av den Internetuppkoppling enkätpersonen har i hemmet. Denna fråga tillhör inte direkt någon frågeställning, utan är en kompletterande fråga till fråga 6.

Fråga 8. Här vill vi undersöka hur länge respondenten är aktivt uppkopplade mot Internet. Det menas hur många timmar i genomsnitt sitter respondenten vid datorn och nyttjar Internet. Detta är en del av vår frågeställning: ”Ökad uppkopplingstid” (se kap 1.2).

Fråga 9. Personer som har fast Internetuppkoppling tenderar att inte koppla ner sig efter de har slutat använda Internet för stunden. Detta innebär att datorn är uppkopplad mot Internet

även om ingen använder Internet. Detta är en del av vår frågeställning: ”Ökad uppkopplingstid” (se kap 1.2).

Fråga 10. Denna fråga har inte direkt någon anknytning till någon speciell frågeställning, utan den har en relevans till flera av våra frågeställningar. Genom att vi skall få en uppfattning om personer med lång datorerfarenhet är mer medvetna om de olika Internetrelaterade säkerhetsrisker och vidtar mer ofta åtgärder mot dessa än personer som har en mindre datorerfarenhet.

Fråga 11. Det ligger i vårt intresse att ta reda på vad privatpersoner använder Internet till. Detta har en stor relevans till vilka Internetrelaterade säkerhetsrisker de utsätter sig för. Till exempel en person som brukar ladda ner musik och program via någon typ av fildelningsprogram, kommer då i kontakt med fler typer av säkerhetsrisker än vad en person som enbart använder Internet för chatta eller surfa. Denna svarar för vår frågeställning: ”Aktiviteter och tjänster på Internet” (se kap 1.2).

Fråga 12. Genom att fråga enkätpersonerna om han eller hon läser någon typ av teknisk datortidskrift regelbundet, kan vi ta reda på om han eller hon borde besitta kunskaper om Internetrelaterade risker och hot. Denna fråga är en del av frågeställningen: ”Säkerhetsmedvetandet hos privatpersoner” (se kap 1.2).

Fråga 13 är en fråga som skall ta reda på hur och med vad respondenten använder sig av för att skydda sig mot Internetrelaterade hot och risker. Denna fråga är en del av frågeställningen: ”Säkerhetsmedvetandet hos privatpersoner” (se kap 1.2).

Fråga 14. Genom att fråga respondenterna om de skulle kunna förklara olika typer av säkerhetsrisktermer som finns på Internet, kan vi få reda på deras medvetenhet om de olika hot som finns kopplat till Internet. Vi formulerade frågan genom att skriva: ”...kunna förklara vad de innebär?”. Istället för: ”...känner till?”. Detta är på grund av att vi vill att enkätpersonerna skall veta innebörden om vad det är hållre än att de bara ha hört termen. Denna fråga är en del av vår frågeställning: ”Säkerhetsmedvetandet hos privatpersoner” (se kap 1.2).

Fråga 15. Med denna fråga vill vi ta reda på hur säkerhetsmedvetna våra respondenter är när de har laddat hem ett program eller en musikfil från Internet. Denna fråga är en del av vår frågeställning: ”Säkerhetsmedvetandet hos privatpersoner” (se kap 1.2).

Fråga 16. Med denna fråga vill vi ta reda på om enkätpersonerna någon gång blivit utsatt för virusangrepp. Denna fråga är en del av vår frågeställning: ”Säkerhetsmedvetandet hos privatpersoner” (se kap 1.2).

Fråga 17. Med denna fråga vill vi ta reda på om enkätpersonerna någon gång blivit utsatt för intrångsförsök. Denna fråga är en del av vår frågeställning: ”Säkerhetsmedvetandet hos privatpersoner” (se kap 1.2).

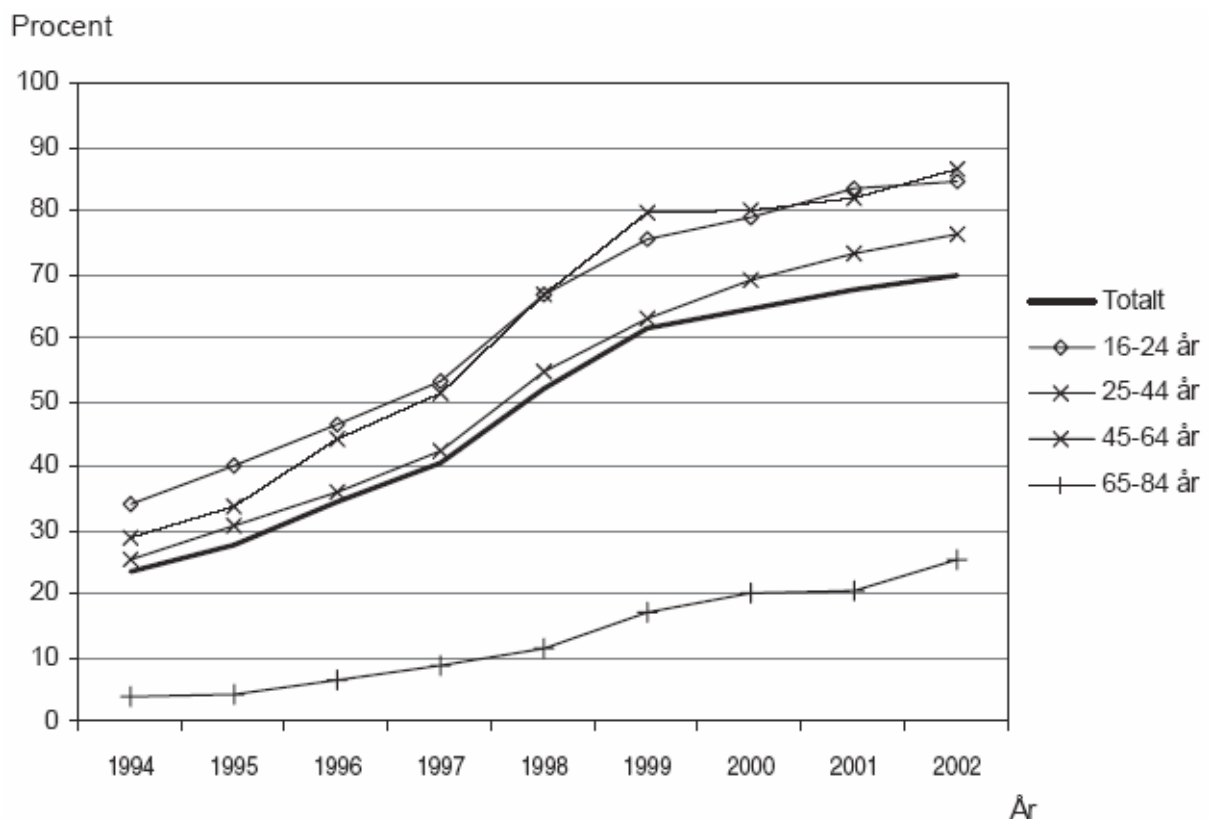
Fråga 18. Genom att fråga en direkt fråga till respondenterna med hjälp av en 5 punkters Likertskala, om hur bra de själva anser sin säkerhet mot Internetrelaterade risker och hot är, kan vi få en bild hur de själva upplever sin säkerhet mot vad de har svarat på våra andra enkätfrågor. Denna fråga är en del av vår frågeställning: ”Säkerhetsmedvetandet hos privatpersoner” (se kap 1.2).

3 Tillgång, användning och säkerhetsproblem av Internetuppkopplade hemdatorer

För att få en bättre bild och se om det har skett några förändringar när det gäller användning av persondatorer, Internet och medvetenhet om säkerhet relaterat till Internet i Sverige är det bra att veta hur det ser ut statistiskt sett från tidigare forskningar. Vi vänder oss då till Svenska Centralbyrån (SCB) för tidigare undersökningar som har gjorts.

3.1 Tillgång till datorer i hemmen

Tillgången till hemdatorer i Sverige har ökat väldigt kraftigt sedan 1994. Enligt SCB var tillgången till hemdatorer år 1994 bara ca 23 procent, för att sedan öka med 47 procent till ca 70 procent år 2002 (se graf 3.1.1) i åldrarna 16-84. Med hemdatorer menas då både stationära och bärbara datorer som finns i hemmen.

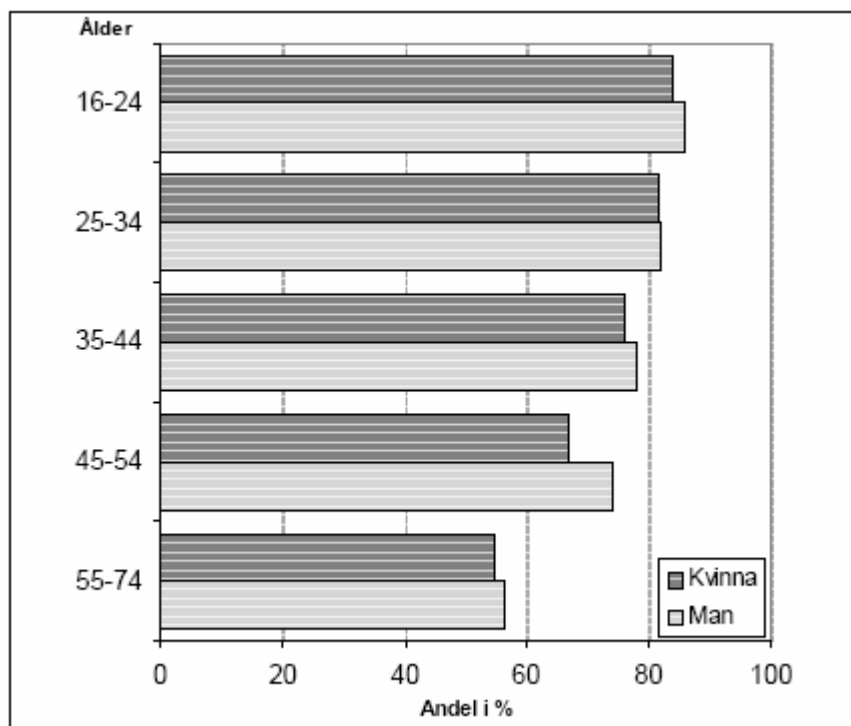


Graf 3.1.1 [SCB 2003, 2004]

Enligt graf 3.1.1 så är det bara ca 25 procent av personer som är 65-84 år gamla som har tillgång till en hemdator år 2002. Detta låga procentantal av de äldre personerna gentemot de andra åldersgrupperna gör att hela snittet för år 2002 blir något mindre.

I en senare undersökning av SCB [Privatpersoners användning av datorer och Internet 2004, 2004, SCB] visade det sig att ca 80 procent av personer mellan 16-74 år har tillgång till en hemdator. Vidare i SCB:s undersökning från 2004 visade det sig att ca 90 procent av de yngre och ca 60 procent av de äldre har tillgång till en hemdator. I denna undersökning visade det sig även att ca 10 procent aldrig använt en persondator. Den största andelen av dessa 10

procent befann sig i den äldre gruppen. Ytterligare framgick det att två av tre använder en persondator varje dag, men bland åldrarna 55-74 så var det dagliga användandet nere i mindre än 50 procent. Det är även en skillnad mellan könen i alla åldersgrupperna, men det är värt att notera att skillnaden är som störst i åldersgruppen 45-54 år (se graf 3.1.2).

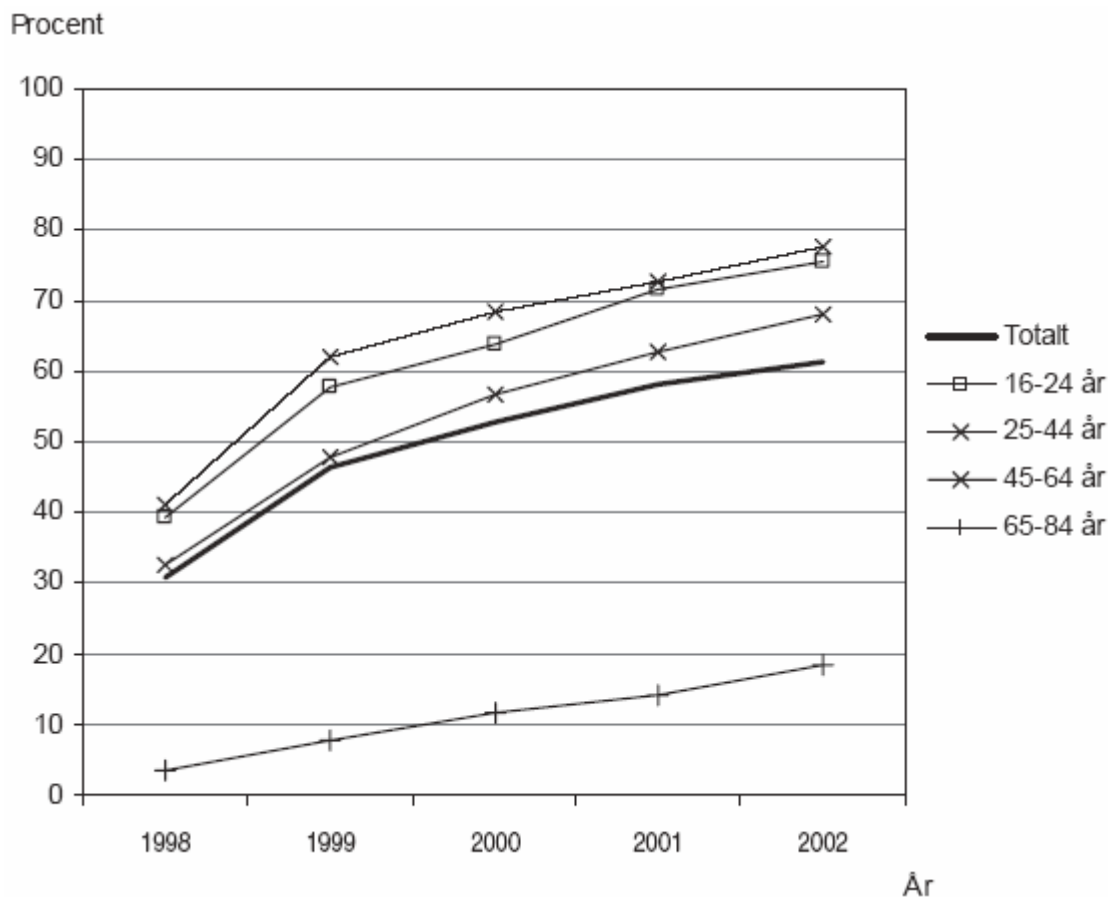


Graf 3.1.2 Andel personer i åldrarna 16-74 år som under första kvartalet 2004 använt en persondator minst en gång per vecka i hemmet. [SCB 2004, 2004]

3.2 Tillgång till Internet i hemmen

Tillgången till en Internetanslutning har även den ökat i takt med ökningen av tillgången av hemdatorer. Första gången SCB gjorde en mätning på tillgången till Internet från hemmet var 1998 och då var ca 31 procent av svenska befolkningen uppkopplad mot Internet från sina hem. För att sedan öka till ca 62 procent 2002 (se graf 3.2.1).

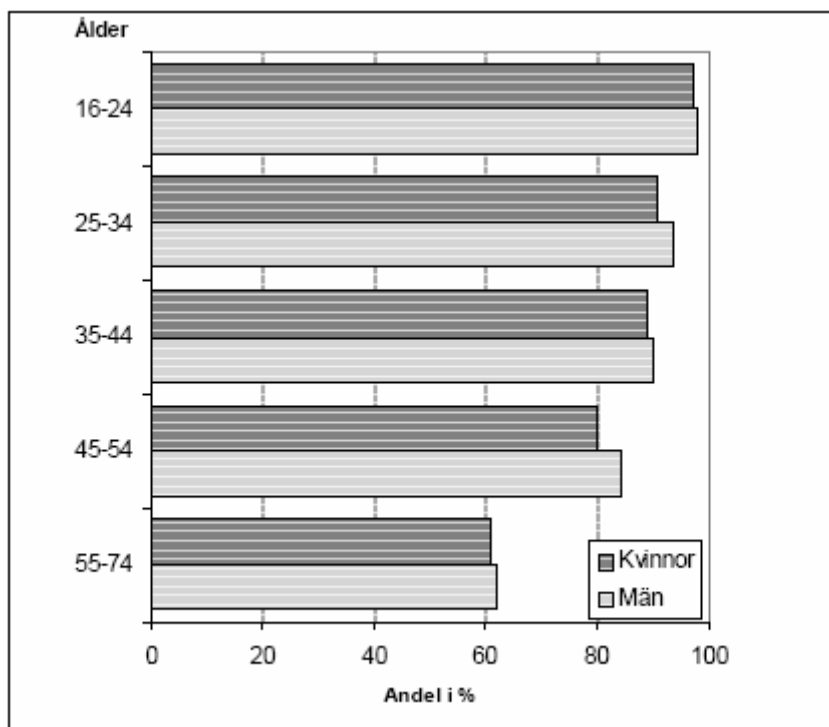
I den senaste undersökningen om privatpersoners tillgång till Internet från hemmet är från första kvartalet av 2004 [SCB 2004, 2004]. I denna mätning gjordes det en undersökning på privatpersoner i åldrarna 16-74 år och deras tillgång till Internet från hemmet, detta inkluderar all typ av Internetuppkoppling som man kan tänkas ha, och inte enbart bara Internetuppkopplade stationära och bärbara datorer. På grund av detta så är procentsatserna något större än om man bara gjorde en undersökning på enbart Internetuppkopplade stationära och bärbara datorer i hemmet.



Graf 3.2.1 (SCB 2003, 2004)

I undersökning från 2004 hade enligt SCB ungefär 80 procent av de tillfrågade, tillgång till Internet i någon form. Ser man på statistiken från SCB:s gruppindelning visade det sig att tillgången sjönk med åldern. I den yngsta gruppen 16-24 år hade ca 90 procent tillgång till Internet medan i den äldsta gruppen 45-64 år hade ca 60 procent tillgång. Bland de yngre använder sig två av tre av Internet och det gör även majoriteten bland de äldre. Skillnaden när det gäller användandet av Internet mellan könen är väldigt små. Det visade sig även att ca var tionde person i undersökningen aldrig använt sig av Internet. I den äldsta åldersgruppen hade var tredje aldrig använt sig av Internet. Av de tillfrågade så använde sig ca hälften av Internet varje dag och enligt SCB så visade det sig att de som var högtbildade i större utsträckning än andra använde sig av Internet varje dag. (Se graf 3.2.2)

Ytterligare visade det sig i undersökningen från 2004 att den vanligaste anslutningen mot Internet var med modem via vanlig telefonlinje. Av de tillfrågade var det ca hälften som anslöt sig på det viset. Det näst vanligaste sättet att ansluta sig var via olika typer av höghastighetsanslutningar. Till höghastighetsanslutningar räknas ADSL (oberoende på vilken överföringshastighet det har), VDSL, kabel TV och lokalt nätverk. Höghastighetsanslutningar fanns i ungefär vart tredje hem och oftast i form av ADSL. Andra sätt att ansluta sig som till exempel med ISDN, satellit eller mobiltelefonen var sällsynta. Om man tittar på könsfördelningen var det vanligare att män kopplade upp sig med höghastighetsanslutningar medan det var vanligare att kvinnor kopplade upp sig med modem via vanliga telefonlinjer.

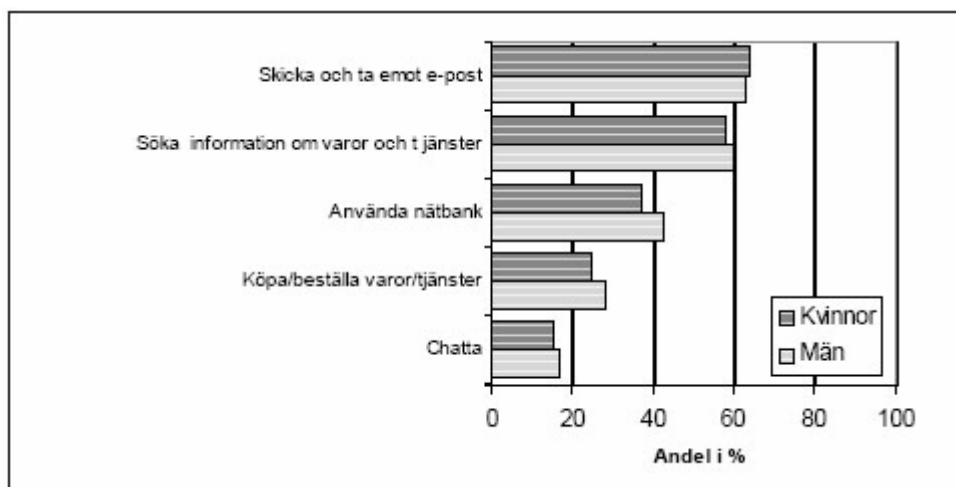


Graf 3.2.2 Andel personer i åldern 16-74 år som under första kvartalet 2004 använt Internet. [SCB 2004. 2004]

3.3 Användning av Internet i hemmen

Internet kan användas till flera olika ändamål och som visas i graf 3.3.1 tillhörde följande aktiviteter och tjänster till de vanligaste ändamålen:

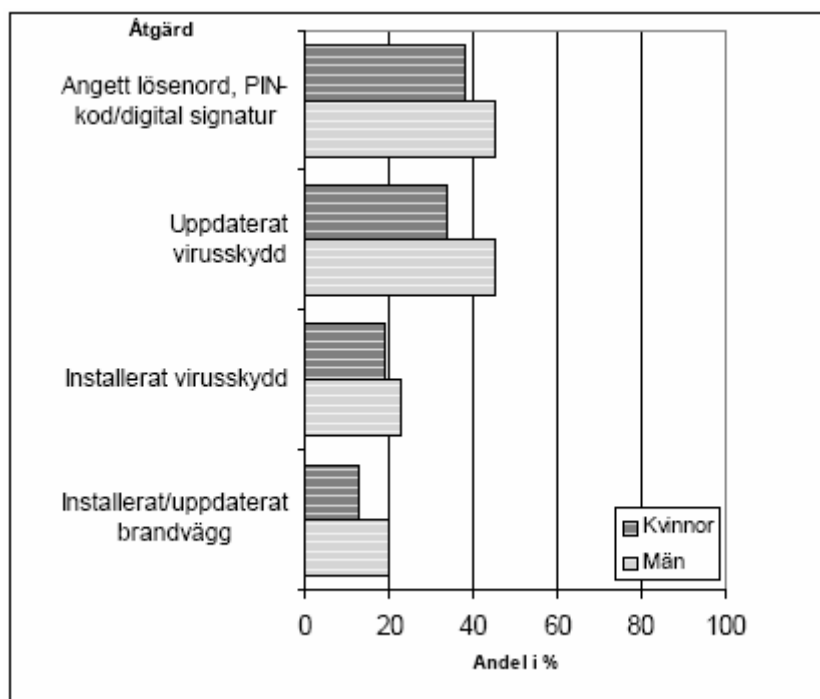
- Skicka och ta emot e-mail
- Söka information om varor och tjänster
- Använda sig av nätbank
- Beställa varor och tjänster
- Chatta



Graf 3.3.1 Andel personer i åldern 16-74 år som under första kvartalet 2004 använt Internet för olika ändamål. [utdrag ur SCB 2004, 2004]

3.4 Säkerhetsproblem vid användning av Internet

Det vanligaste säkerhetsproblemet som folk drabbats av enligt undersökningen är Datavirus. Av de undersökta hade ungefär var femte person drabbats av det. De personer som drabbades oftast var de i den gruppen där Internetanvändning var stor. Ett annat problem som undersökningspersonerna råkat ut för var bedrägeri vid betalning, men det var väldigt ovanligt. Bara ca en procent av de tillfrågade hade råkat ut för det. Fem procent av de tillfrågade hade råkat ut för att konfidentiell information som skickas över nätet hade missbrukats. Ett problem som var vanligt bland de personer som blivit undersökta var Spam det vill säga oönskade e-mail. Det hade ca var tredje person råkat ut för. De personer som vanligast råkade ut för Spam var män med gymnasial eller eftergymnasial utbildning.



Graf 3.4.1 Andel personer i åldern 16-74 år som under första kvartalet 2004 vidtagit säkerhetsåtgärder för den egna persondatorn. [SCB 2004. 2004]

I SCB:s undersökning fanns ingen statistik över hur många som till exempel hade drabbats av intrångsförsök, och på vilket sätt de drabbats, på sin persondator i hemmet eller på vilket/vilka sätt en person skyddar sin persondator i hemmet mot olika sorters attacker. Det är den informationen som vi vill få ut från vår undersökning, eftersom den inte finns med i SCB:s undersökningar.

4 Säkerhetsrisker

Den ökande takten av Internetuppkopplade hemdatorer innebär ett växande säkerhetsproblem, framförallt genom det växande antalet fasta anslutningar med hög kapacitet och att uppkopplingstiden mot Internet ökar.

Att skydda sina datorer mot olika typer av Internetrelaterade hot har alltid varit en självklarhet hos företagen, men inte hos privatpersonen. Detta håller på att förändras, eftersom folk i allmänhet blir mer medvetna om dessa olika typer av Internetrelaterade hot. Det är dock fortfarande en väldigt liten andel privatpersoner som aktivt skyddar sina hemdatorer mot Internetrelaterade hot (se graf 3.4.1 i föregående kapitel).

Vad är då ett hot? I observationsrapporten 21/2000 ”Säkerhet på Internet – Datavirus och blockering av tjänster” skriven av Observatoriet för informationssäkerhet definierar ordet hot på ett bra allmänt sätt:

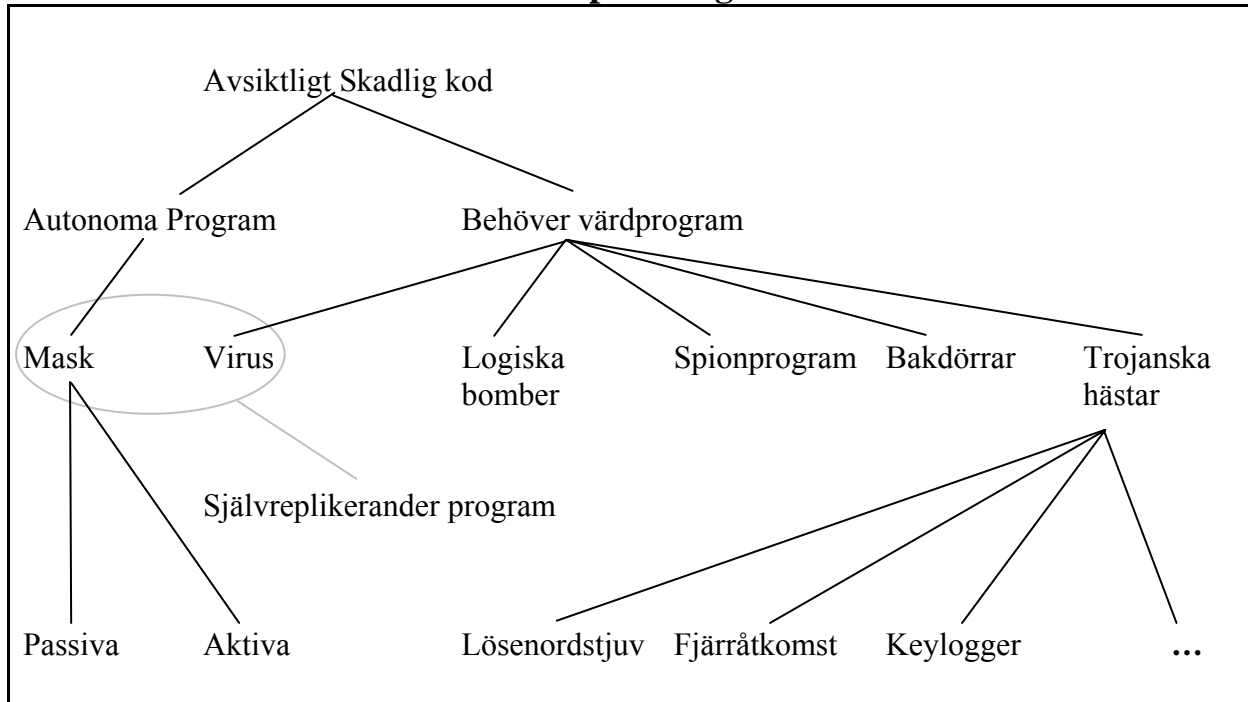
”Ett hot definieras som en möjlig, oönskad händelse som ger negativa konsekvenser för någon. Risk är sannolikheten för att en oönskad händelse skall inträffa. Dvs. det faktum att det finns ett hot innebär inte med automatik att man behöver drabbas av det. Utgående från en riskbedömning kan man anpassa skyddet.”

4.1 Skadlig kod

Begreppet virus är ett namn som många använder lite slarvigt på kod som oftast har till syfte att göra något oönskat eller oväntat på en dator. Men i och med att allt inte är ”virus” kan det ibland vara bra att veta skillnaden mellan virus (Datavirus) och andra obehagliga existerande företeelser. Det som är gemensamt för de olika företeelserna som folk i daglig mun kallar för ”virus” är att det är skadlig kod. När vi nämner ”virus” med situationstecken syftar vi på någon form av skadlig kod. Denna skadliga kod kan utföra allt från ett lättsamt skämt till att förlora all information i datorn. [Observatoriet för informationssäkerhet, 2000]

De olika företeelserna av skadlig kod kan spridas på olika sätt. Datavirus sprids oftast när man utbyter information eller laddar hem olika program. Med utbyte av information menas till exempel att Dataviruset är gömt i en bifogad fil som kommer med e-mail. För att en trojan ska kunna spridas måste den hämtas eller överlämnas av något program. Maskar sprider sig genom att sända iväg sig själv via till exempel e-mail eller chat och installerar sig själv på mottagarens dator. Hur snabbt ett ”virus” sprider sig beror på vilken typ av program och datormiljö det befinner sig i. Ytterligare en faktor som påverkar hur snabbt det sprider sig är vilka egenskaper det har utrustats med.

Släktskap skadlig kod



Graf 4.1.1 (ROMAB, 2005)

Hur mycket skada ett "virus" utföra för en användare beror på vilka avsikter det har samt hur snabbt man upptäcker attacken. Som vi nämnt tidigare har ett "virus" ett brett register på vad det kan utföra. Bland de vanligaste syftena med ett "virus" är:

- Förändra information
- Stjäla lösenord
- Ge sig själv och andra tillträde till information
- Förstöra information
- Skicka sig själv vidare till andra till exempel genom att sprida sig till alla som finns i ens e-mails adressbok.
- Datorn blir långsammare
- Datorn hänger sig
- Datorn kraschar och/eller startar om sig med jämna mellanrum
- Använda din dator som lagringsplats
- Använda din dator till att attackera andra

Men de flesta "virus" som sprids över Internet utför inte någon större skada överhuvudtaget. Fast däremot så ger de skada på så sätt att de är irriterande för användaren samt att användaren läger ner massa tid på att försöka ta bort dem. [Microsoft, 2005] [Observatoriet för informationssäkerhet, 2000]

Störst risk för att drabbas av något slags "virus" har de som ofta är anslutna mot Internet och laddar ner mycket program eller information, speciellt om man inte riktigt vet varifrån de kommer.

Nedan beskrivs kort de vanligaste typerna av skadlig kod vilket är Datavirus, Maskar och Trojaner.

4.1.1 Datavirus

Datavirus, eller virus som man oftast säger, ökar över åren i en oförutsägbar takt. Historiskt sett enligt rapporten *Observatorierapporten 23/2000*, så fanns det 1986 ett känt Datavirus. Tre år senare kände man till sex stycken och år 1990 hade det ökat till 80 stycken. Från december 1998 till oktober 1999 ökade de kända virusen från ca 20 500 stycken till ca 42 000 stycken. Idag finns över 50 000 stycken virus.

Nu förtiden är det vanligast att virus sprids över Internet och då framförallt via e-mail. Tidigare var det vanligast att de spreds via disketter eller någon annan typ av flyttbar media.

Men vad är då ett Datavirus? Ett Datavirus är en självständig del av ett program som kan döljas i ett annat program. Instruktionerna för viruset utförs sedan inte förrän programmet där det ligger gömt aktiveras. Viruset smittar sedan den miljön där det inplanterats. Detta sker genom att det kan kopiera sig själv och sedan infektera andra filer i sin omgivning. [Observatoriet för informationssäkerhet, 2000] [Axelsson, 2001] [Secure-IT, 2005]

Det finns även så kallade falska virus, Hoaxvirus, som är ett e-mail som har för avsikt att skrämja användaren att han/hon drabbats av ett icke existerande virusshot. Det vill säga att det är ett informations e-mail där det varnas för farliga e-mail meddelande med en viss rubrik. Denna typ av informations e-mail uppmanas sedan användaren att skicka det vidare till vänner och bekanta. [Observatoriet för informationssäkerhet, 2000]

Problemet med dessa är att det oftast tar mer tid att hantera denna typ av varningar än att ta hand om riktiga ”virusattacker”. Med andra ord läggs det ner mycket resurser på falska virus, vilket kostar massor av pengar. Förutom de resursmässiga problemen medför även falska virus även trafikmässiga problem på Internet. [ibid]

4.1.2 Maskar

En annan typ av skadlig kod är Maskar (Worms). Till skillnad från till exempel Datavirus är inte en Mask beroende av att dölja sig i ett annat program. Det beror på att en Mask är ett självständigt program som kan existera för sig själv. Precis som Datavirus kopierar Maskar sig själva för att spridas så fort som möjligt. Det kan medföra att Masken breder ut sig i hela nätverket vilket kan leda till att tillgängligheten till datorn minska och det kan medföra att belastningen blir så stor att inga andra program kan fungera. Maskar sprids vanligast via e-mail för att kunna infektera så många datorer som möjligt. [Observatoriet för informationssäkerhet, 2000] [Post och Telestyrelsen, 2005] [Microsoft, 2005]

4.1.3 Trojan/Trojansk häst

Begreppet Trojan eller Trojansk häst härstammar från Homeros litterära verk Iliaden där grekerna tog sig in i staden Troja med hjälp av en stor trähäst. Men vad har då denna historia med trojan i IT sammanhang att göra? En Trojansk häst i IT-sammanhang är en dold del där den skadliga koden kan finnas i ett program eller i en bit kod, men som verkar helt ofarlig. Denna dolda del, som verkar helt ofarlig, kan innehålla ett Datavirus eller någon annan form av otrevlig programkod. En Trojan kan vara konstruerad på så sätt att den raderar ut sig själv och sopa igen alla spår efter sig när skadan väl är skedd. [Observatoriet för informationssäkerhet, 2000] [Post och Telestyrelsen, 2005] [Microsoft, 2005]

4.1.4 Bakdörr (Trapdoor)

En Bakdörr kan ses som en ”hemlig” ytterdörr i ett hus. När man väl känner till denna bakdörr så har man full access till hela huset. Samma sak gäller för en Bakdörr i datasammanhang, en alternativ väg för att få full kontroll över datorn. Med det kan man säga att en Bakdörr tillåter någon att få access till datorn utan att gå igenom de vanliga säkerhetsprocedurerna. Oftast använder sig programmerare av bakdörrar för att testa olika programmoduler under utveckling av ett datorsystem. [Stallings, 2000]

De som utvecklat ett system tar vanligtvis bort Bakdörrarna när testerna är klara. Men ibland görs inte detta vilket kan bero på flera olika faktorer. Bland annat kan det bero på:

- Glömt att ta bort dem
- Avsiktligen lämnat dem kvar för att göra framtida tester
- Avsiktligen lämnat dem kvar för att kunna göra intrång när programmet kommit i drift.

[Pleeger, 2003]

Bakdörrar kan även komma in i datorn på andra sätt som till exempel via någon typ av skadlig kod. Kommer någon obehörig in via en Bakdörr kan han/hon utnyttja den som ett fjärstyrningsverktyg eller liknande. [F-Secure, 2003]

4.2 Portskanning

När en som vill göra intrång i en annans dator har hittat sitt mål kan han/hon göra en Portskanning. Om han/hon tycker att det är potentiellt mål skannar personen oftast alla 1 024 välkända (Well-Known) portar i TCP och alla 1 024 välkända portar i UDP. [Panko, 2003]

Portskanning går till på sådant sätt att den personen som vill göra intrång i en annans dator skannar alla de välkända portarna på måldatorn, för att identifiera vilka tjänster som är aktiva. Dessa eventuella tjänster som körs på måldatorn kan attackeras på olika sätt genom att hitta olika kryphål i dessa och ta fördelar av dessa. [Panko, 2003]

4.3 Spam

Spam eller skräppost kan förklaras som massutskick med meddelande via Internet. Var ordet Spam kommer ifrån finns det egentligen ingen direkt förklaring till. Dessa meddelanden är oftast reklam för olika företag eller tjänster som den som får dem oftast inte har bett om eller är intresserade av. Det finns lite olika sätt hur företagen som gör utskicken får tag på adresserna som de skickar till. Till exempel får de adresserna via databaser, sökningar via Internet, nyhetsgrupper och liknande. [Microsoft, 2005] [Axelsson, 2001]

Problemet med Spam, förutom att de kan innehålla virus eller något liknande, är att oftast det att det skickas ut i enorma mängder, vilket leder till stora belastningar på servrar och routrar över Internet. [Microsoft, 2005]

Ett misstag som många användare gör är att öppna skräppostmeddelanden. Genom att göra detta bekräftar du för dem som skickar ut meddelandena att din e-mailadress fungerar vilket oftast leder till att du bara får fler. [ibid]

Spam känns oftast igen genom att meddelandet kommer från ett okänt företag. Deras adress, e-mail och telefonnummer är oftast påhittade och att meddelandet innehåller stavfel eller annan konstig grammatik såsom enbart versaler och många utropstecken. [ibid]

4.4 Spionprogram (Spyware) och liknande

När en person använder sin Internetuppkopplade dator kan denna person ha Spyware i sitt system genom att det har blivit installerat i samband med något annat program. Det är vanligt att mindre seriösa företag samlar in information om användaren på detta sätt, vilket leder till att den personliga integriteten kränks. Att personlig integritet kränks menas att personlig och privat information delges eller behandlas av andra personer utan samtycke eller vetskap. [Post och Telestyrelsen, 2005] [Microsoft, 2005]

Begreppet Spionprogram används vanligtvis när integritetskränkande program kommer på tal, men begreppet saknar dock en entydig definition. Ett Spionprogram behöver inte vara ett program som exekveras på en användares dator utan kan till exempel vara en enkel textfil. Det ska dock förtydligas att alla Spionprogram inte behöver vara integritetskränkande, de kan även ha andra funktioner och syfte. [Post och Telestyrelsen, 2005]

Ett sätt att dela in Spionprogram i olika kategorier är att dela in dem såsom Post och Telestyrelsen har gjort. De har delat in dem i tre olika kategorier, baserat på Spionprogrammets användningsområde. Den första kategorin är spionprogram som används för reklam och marknadsföring (Advertising Spyware). Den andra kategorin är Spionprogram som används för informationsinsamling och den sista gruppen är Spionprogram som används för att kunna fjärrstyra och övervaka datorer (Surveillance Spyware). Givetvis kan ett Spionprogram vara en blandning mellan de tre kategorierna. [Post och Telestyrelsen, 2005] [Incabus System, 2004]

4.5 Hacker och cracker

Man kan grovt kategorisera de personer som ligger bakom de flesta olika typerna av säkerhetshot till två typer, Hacker och Cracker.

4.5.1 Hacker

Företeelsen Hacker dök upp på 1960 talet i Massachusetts Institute of Technology, förkortat MIT, och hade ingenting att göra med datorer. Definitionen av en Hacker på MIT var en person som aldrig gick i skolan, sover hela dagarna och spenderar nätterna igenom med att fullt tillägna sin tid med någon typ av hobby. 1986 fick ordet hacker en lite annorlunda betydelse på MIT, nämligen en person som utforskade olika typer av områden på skolan där han eller hon inte fick lov att vara (hackade sig in), detta kunde vara skolans tak eller service-tunnlarna under skolan. [Harvey, 2005]

Dagens definition av en Hacker har funnits några år och beskriver en person som lever för datorer och allt han eller hon gör har någonting med datorer att göra. Vidare så är personen väldigt kunnig med datorer och kan oftast massor med olika programmeringsspråk. Något som är lika viktigt när man definierar en Hacker är hans eller hennes attityd. Hackern måste

ha sin dator som en hobby, någonting som han eller hon tycker är kul att hålla på med, inte någonting som han eller hon måste göra eller för att tjäna stora pengar. [ibid]

4.5.2 Cracker

En Crackers definition är oftast närbesläktad av en Hacker. Båda är väldigt skickliga och kunniga med datorer. Den stora skillnaden mellan en Cracker och en Hacker är deras attityd till varför de spenderar sin tid åt datorer. En Hackers attityd beskrivs i kapitlet ovanför. En Crackers attityd är en person som ägnar sina kunskaper till att förstöra och stjäla, allt för att ställa till besvär eller att tjäna stora pengar. Man kan säga att en Cracker kan ses som en professionell brottsling. [Harvey, 2005] [Indiana University, 2005]

Det skall tilläggas att de flesta Crackers inte är lika datokunniga som Hackers. Crackers är mer specialiserade på ett eller ett fåtal saker, till exempel han eller hon kan vara väldigt duktig på att veta hur man knäcker lösenord eller tar sig förbi olika säkerhetssystem. [Harvey, 2005] [Indiana University, 2005]

5 Skydd

Att skydda sin dator mot olika typer av hot har alltid varit viktigt. För några decennier sedan så var det mest olika typer av fysiska hot man skyddade sig mot. Mitten av 80 talet började förekomsten av Internet (Newsgroups) bli allt vanligare. Detta ledde till att man började sprida programvara, vilket också medförde uppkomsten av de första Datavirusen. Några år senare började de första antivirusprogrammen dyka upp på marknaden.

Situationen just nu är att allt fler kopplar upp sig mot Internet med olika typer av bredbandslösningar. Detta i sin tur leder till att uppkopplingstiden ökar drastiskt, och att enbart skydda sig med ett antivirusprogram räcker oftast inte till. Därför finns det en mängd olika sätt som man kan skydda sin hemdator på. I detta kapitel förklarar de vanligaste sätten man kan skydda sin hemdator på.

5.1 Brandvägg

En brandvägg i ett hus är en vägg som skall stoppa spridningen av en eventuell brand för att nå från det ena rummet till det andra rummet. En Brandvägg i datorsammanhang har i princip samma syfte, den skall stoppa oönskad information att sprida sig mellan datorer, till exempel en hemdator som är uppkopplad mot Internet behöver skyddas.

En Brandvägg har två extrema lägen, helt öppen eller helt stängd. Om den är helt stängd kan ingen komma in och ingen kan komma ut och om den är helt öppen kan alla komma ut och vem som helst kan komma in. Det svåra med en Brandvägg är att konfigurera den rätt, så exakt den trafik som behövs får passera ut och in genom den.

Det finns en mängd olika typer av Brandväggar i datorsammanhang, men den typen av Brandvägg som oftast används av privatpersoner är den så kallade *personliga brandväggen*. Denna typ av Brandvägg består av ett mjukvaruprogram som körs på hemdatorn. Dess uppgift är att blockera all trafik som inte är önskvärd. Konfigurationen består av att man har en "white" lista och en "black" lista. I "white" listan har man adresser på trafik som är tillåten, och i "black" listan har man trafik som man inte tillåter. Detta kan bestå av både IP-nummer och portnummer. Man kan även ställa in olika säkerhets nivåer, till exempel dessa adresser litar jag blint på, medan andra adresser bara kan skicka information, inte begära information. [Pfleeger & Pfleeger, 2003]

5.2 Antivirusprogram

Det finns en hel uppsjö med olika typer antivirusprogram, som till exempel McAfee, Norton Antivirus, F-Secure mm. Alla dessa olika typer av program har en gemensam uppgift, att skydda datorn mot olika typer av virusangrepp. Men vad är då ett antivirusprogram? Det är ett mjukvaruprogram som letar efter virus på hårddisken eller i datorns minne för att sedan försöka ta bort viruset. De flesta antivirusprogrammen kan automatiskt uppdatera sitt virusbibliotek för att alltid kunna upptäcka de senaste virusen.

5.3 Användarpolicy

Genom att ha olika typer av regler i ett hushåll där flera personer har tillgång till den Internetuppkopplade datorn. Självklart kan man som ensam datoranvändare ha sin egen användarpolicy. Dessa regler kan bland annat bestå i att man inte besöker vissa typer av hemsidor, eller alltid ser till en extra gång att olika typer av säkerhetsprogram är aktiva när man kopplar upp sig mot Internet.

5.4 Krypteringsprogram

All information som sänds på Internet kan vem som helst på ett enkelt sätt avlyssna. En privatperson eller ett företag som behöver sända känslig information genom Internet, är mån av att denna information inte plockas upp av någon obehörig.

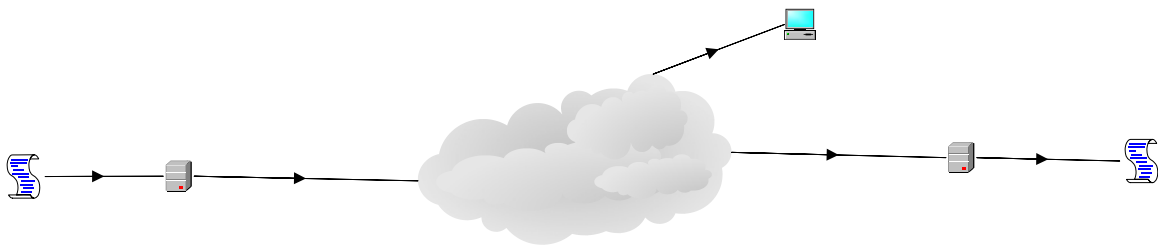


Bild 5.4.1 (Källa: Egen)

Genom att kryptera informationen man sänder, förhindrar man obehöriga att ”tjuvlyssna” på trafiken, då kan det se ut som följande bild under:

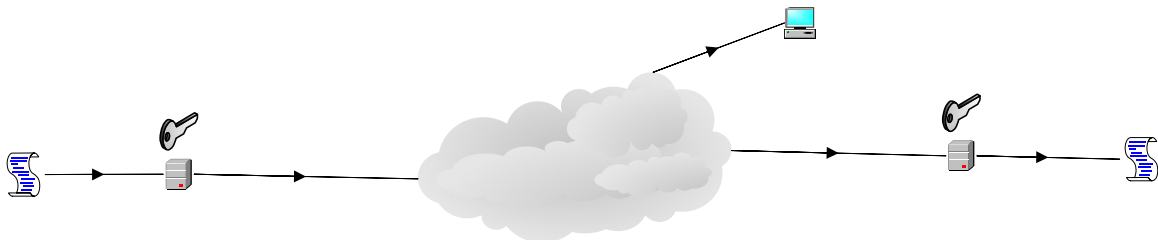


Bild 5.4.2 (Källa: Egen)

Det kan även vara aktuellt att man krypterar information på sin egen dator, utan att ha som avsikt att skicka iväg informationen till någon. Detta på grund av att man vill vara säker på att den informationen man har på sin dator skall vara helt säker, det finns alltid en risk att någon hackar sig in i datorn, eller att någon rent fysiskt kommer åt datorn. [Axelsson, 2001]

5.5 Filtreringsprogram som hindrar besök på osäkra sidor

CyberPatrol och Net Nanny är de mest kända program som har möjligheten att hindra besök på olika typer av hemsidor. Genom att ställa in dessa program på att blockera vissa typer av sidor, då kommer det att bli omöjligt att besöka dessa sidor från den datorn där ett sådant program är installerat. Sidor som är vanligast att blockera är till exempel: pornografiska, rasistisk propaganda och olika typer av sidor där man kan till exempel tillverka bomber. [Net Nanny, 2005]

I dessa program kan man blockera allt från en specifik adress till att specificera olika typer av ord. Genom att specificera olika ord, då kan dessa program blockera besök på en sida som innehåller de orden man har specificerat. [Net Nanny, 2005] [CyberPatrol, 2005]

5.6 Säkerhetsuppdateringar

När ett operativsystem kommer ut på marknaden, så kvittar det hur mycket tillverkarna av operativsystemet har ansträngt sig för att förhindra att deras operativsystem inte innehåller några säkerhetsbrister. Detta på grund av att det finns alltid såkallat hackers och crackers (läs mer om hackers och crackers i föregående kapitel) som tillägnar all sin tid att upptäcka olika vägar att ta sig in i ett operativsystem. Detta medför att tillverkaren av operativsystemet måste möta upp dessa nyupptäckta säkerhetsbrister genom att stänga dessa intrångsvägar.

Som användare måste man konturenligt uppdatera sitt operativsystem mot nyupptäckta säkerhetsbrister. *Windows Update* är det vanligaste uppdateringstjänsten för att säkerhetsuppdatera *Microsofts* operativsystem.

6 Enkätanalys

6.1 Utförande

Som vi skrev i kapitel 2.5 (Urval), var vi tvungna att ändra urvalet på de respondenter som skulle besvara vår enkät. Vårt första val var att använda oss av ett stickprovsurval.

Stickprovsurvalet bestod av att vi gick till Malmö station och slumpvist valde ut respondenter från de personer som satt och väntade på sina tåg. Vi trodde detta skulle vara en bra idé, eftersom vi förmodade att de personer som satt och väntade skulle ha tid med att besvara vår enkät. Något som vi missade var att förutse deras vilja att besvara vår enkät. Det visade sig att folk i allmänhet varken var intresserade eller orkade ta tiden att besvara våra enkäter. Detta misslyckade stickprovsurval på Malmö station resulterade i endast två besvarade enkäter utav trettio förfrågade personer.

Eftersom vår första metod av urval till vår enkätundersökning fallerade, var vi tvungna att göra en ny undersökning. På grund av tidsbrist hade vi inte tid att utforska andra typer av lämpliga metodurval, och valde därför att göra en bekvämlighetsurvalsundersökning.

En bekvämlighetsundersökning är inte det bästa valet om man vill få en bra spridning på svarspopulationen vilket kommer att återspeglas i hela vår analys och resultat-diskussion.

6.2 Analys av enkätfrågorna

Vår stickprovsurvalsundersökning resulterade i 2 besvarade enkäter utav 30 förfrågade personer. Detta gav oss en svarsfrekvens på under 7%. Bekvämlighetsurvalsundersökningen resulterade i 29 besvarade enkäter utav 29 utdelade enkäter, vilket gav oss en svarsfrekvens på 100%.

Totalt fick vi in 31 besvarade enkäter utav 59 förfrågade personer, och detta gav oss en svarsfrekvens på 53% och ett bortfall på 47%.

Fråga 1 - Könsfördelning

Av de 31 besvarade enkäter var det 15 män och 16 kvinnor. Den jämna könsfördelningen var inget vi hade i åtanke när vi gjorde vår undersökning.

Fråga 2 - Åldersgrupper

Åldersfördelningen av respondenterna är jämt fördelade över de olika åldersgrupperna. Något som är värt att notera är att åldersgruppen 45-54 år har endast kvinnliga respondenter (diagram 6.2.1).

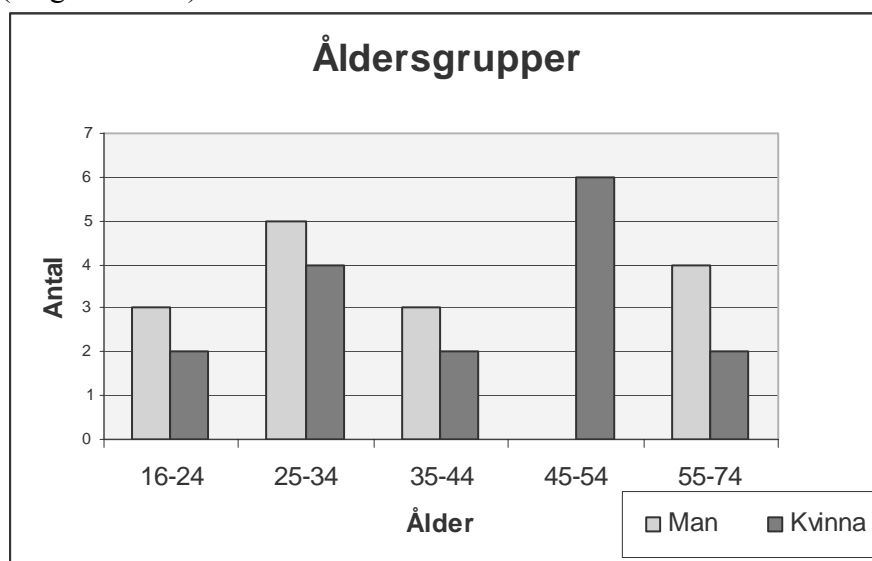


Diagram 6.2.1 [Källa: egen]

Fråga 3 – Utbildningsnivå

Fråga 3 i vår enkät frågade vi efter respondenternas högsta avslutande utbildningsnivå.

Av de 31 svarande hade endast 3 stycken grundskola, 8 stycken gymnasial och hela 20 stycken hade någon form av avslutad eftergymnasial utbildning.

Fråga 4 – Tillgången till en Internetuppkopplad hemdator

Av de 31 svarande hade 28 tillgång till en Internetuppkopplad hemdator. Det är dessa 28 respondenterna som vi kommer att fortsätta denna enkätanalys på, eftersom de 3 respondenterna som inte hade någon tillgång till en Internetuppkopplad hemdator inte är intressanta för vår undersökning. (Om det inkluderar respondenter som inte har någon Internetuppkopplad hemdator kommer detta att anges i vår resultat-diskussion.)

Fråga 5 – Hur betalar du för er Internetuppkoppling?

Hela 23 av de svarande angav att de betalar en fast avgift för att användandet av Internet från hemmet. 5 respondenter angav att deras betalning berodde på uppkopplingstiden. Ingen av respondenterna angav att deras betalning för användandet av Internet berodde på hur mycket de laddade ner. Något som är intressant är att fler män än kvinnor betalade en fast avgift för användandet av Internet från hemmet (13 män, 10 kvinnor) och att det var fler kvinnor än män som angav att deras betalning berodde på hur länge de var uppkopplade mot Internet (1 man, 3 kvinnor).

Fråga 6 – Vilken typ av uppkoppling har du i hemmet?

På frågan om hur respondenterna kopplar upp sig mot Internet svarade 13 respondenter att de kopplade upp sig via ADSL. Antalet respondenter som kopplade upp sig via modem eller hade en fast anslutning var lika stor, men könsskillnaderna mellan dem skiljer sig (diagram 6.2.2).

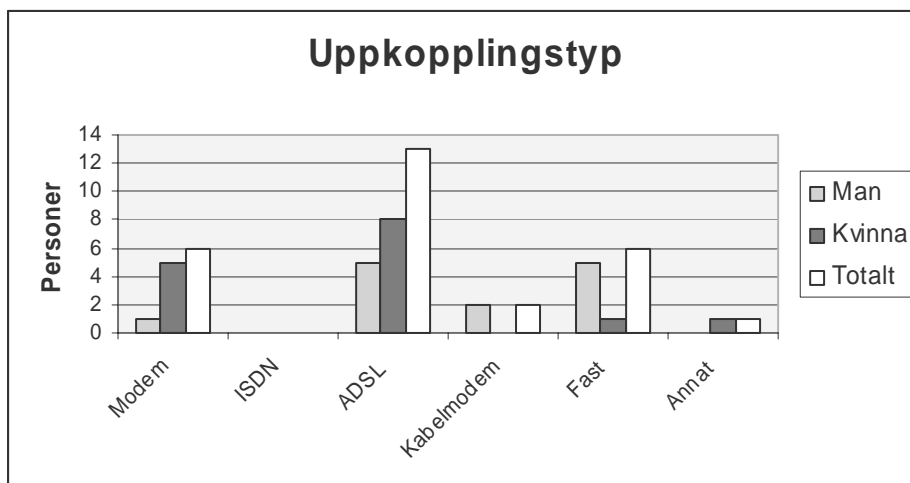


Diagram 6.2.2 [Källa: egen]

Fråga 7 – Vilken är den främsta orsaken till ditt val av uppkoppling i hemmet?

Det vanligaste svarsalternativet (11 stycken) var alternativet ”annat”. Efter det kom svarsalternativet ”ekonomiska skäl” som 7 stycken svarade. Något som var värt att notera var att ingen av våra respondenter angav att deras val av uppkoppling berodde på säkerhetsskäl.

Fråga 8 - Hur länge är du aktivt uppkopplade mot Internet under ett genomsnittligt dygn?

Flertalet av respondenterna (22 stycken) svarade att de sitter som längst upp till 4 timmar framför datorn. Endast 6 stycken, vilket visade sig enbart vara män, svarade att de sitter framför datorn i mer än 4 timmar.

Fråga9 - Hur länge brukar er hemdator vara uppkopplad mot Internet?

Det vanligaste svaret från respondenterna (5 män, 8 kvinnor) var att de endast var uppkopplade medan de sitter framför datorn. Nästan lika vanligt var svaret att de var uppkopplade under dagtid som 10 stycken svarade (5 män, 5 kvinnor). Endast 5 stycken svarade att de alltid var uppkopplade och av dessa var 4 stycken män och 1 kvinna.

Fråga 10 - Hur många års erfarenhet med datorer har du?

Mer än hälften av de svarande angav att de har 6 eller fler års datorerfarenhet. Endast 1 respondent hade väldigt liten datorerfarenhet.

Fråga 11 - Vilken/vilka aktiviteter och tjänster använder du på Internet?

De två vanligaste aktiviteterna eller tjänsterna som respondenterna använder sig av på Internet är att e-maila och söka information (25 stycken vardera). Efter dessa båda kommer banktjänster med 21 stycken svar och därefter kommer att beställa varor och tjänster med 20 stycken svar (diagram 6.2.3).

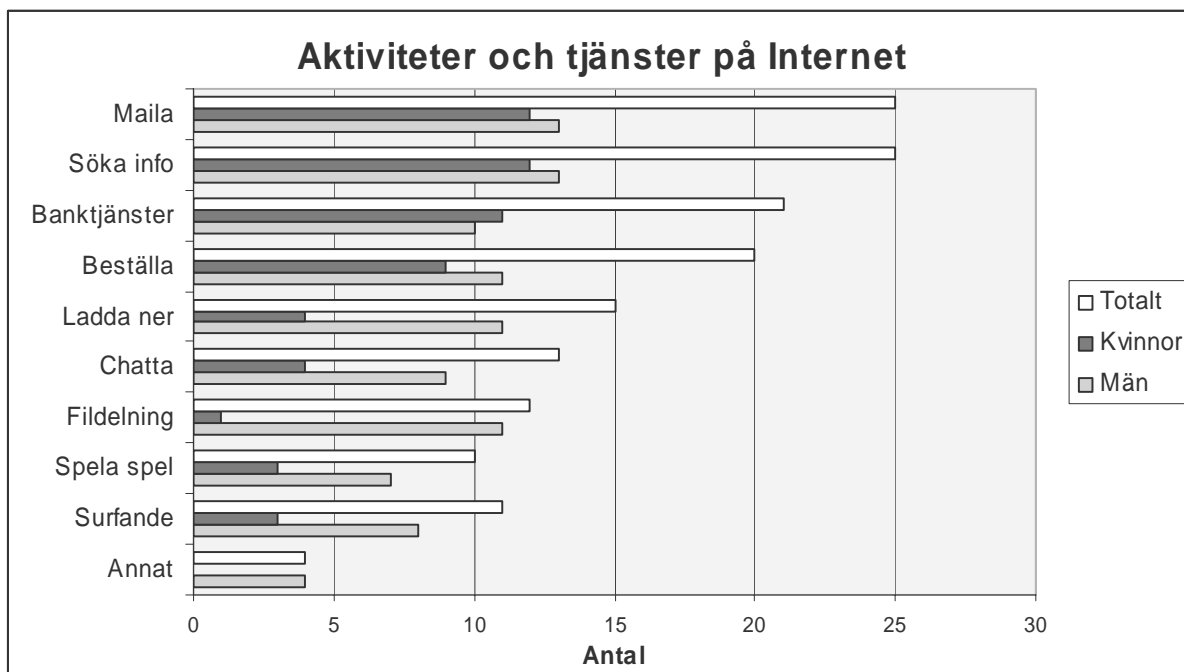


Diagram 6.2.3 (Källa: egen)

Fråga 12 - Läser du regelbundet någon typ av teknisk datortidning?

Av våra 28 svarande respondenter var det endast 2 stycken som regelbundet läser någon typ av teknisk datortidning som till exempel Computer Sweden. Båda respondenterna visade sig vara män.

Fråga 13 - Vilket/Vilka av nedanstående säkerhetsåtgärder använder ni för att skydda er hemdator?

Det vanligaste sättet att skydda sin dator var att använda någon typ av antivirusprogram, vilket 75% av de svarande (28 stycken) använde sig av. Ungefär 50% av de svarande använder sig av någon typ av Brandvägg, samt ser till att de har de senaste säkerhetsuppdateringarna till sitt operativsystem (diagram 6.2.4).

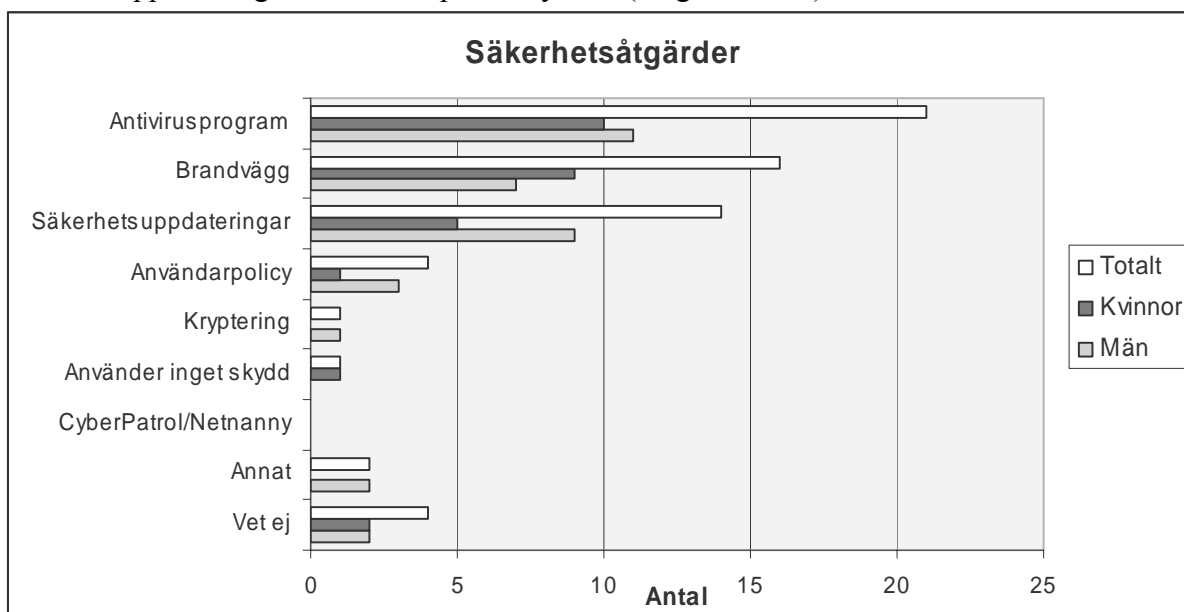


Diagram 6.2.4 (Källa: egen)

Fråga 14 - Vilket/vilka säkerhetsrisker skulle du kunna förklara vad de innebär?

När det gäller olika säkerhetsrisker en datoranvändare kan råka ut för visade det sig att män i större utsträckning än kvinnor kunde förklara vad de dessa innebar. Trojaner var den säkerhetsrisk som flest respondenter kunde förklara vad det innebar. Noterbart är också att ingen kvinna kunde förklara vad Netbus eller Portskanning var (diagram 6.2.4).

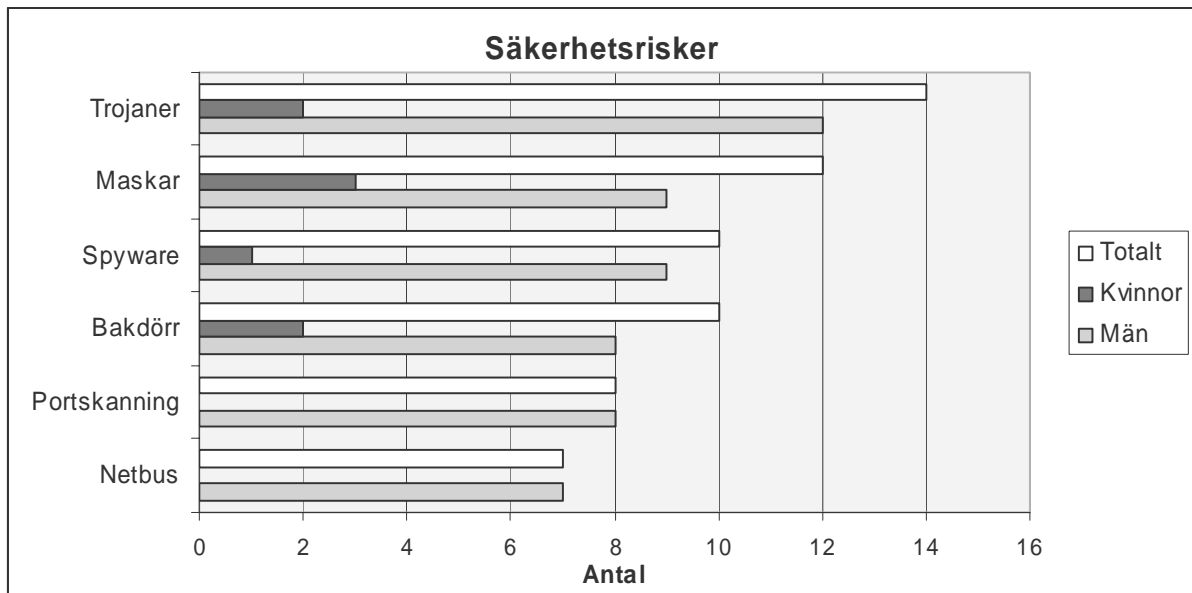


Diagram 6.2.4 (Källa: egen)

Fråga 15 - Vad gör du om du har laddat hem ett program eller en musikfil?

Det vanligaste svaret (9 stycken) som respondenterna angav när de har laddat ner ett program eller en musikfil från Internet, är att de ser till att deras antivirusprogram är aktivt innan de kör eller lyssnar på filen. Det näst vanligaste (6 stycken), var att inte gör någonting alls, utan bara kör eller lyssnar på filen direkt. Nästan en tredjedel av de kvinnliga respondenterna laddade inte hem någon typ av program eller musik fil från Internet.

Fråga 16 - Har din hemdator någon gång blivit utsatt för ett virusangrepp?

Cirka hälften av respondenterna svarade att deras hemdator hade blivit utsatt för virusangrepp. 6 stycken svarade att de inte visste om de hade blivit angripna medan 5 stycken svarade att de inte hade blivit det.

Fråga 17 - Har din hemdator någon gång blivit utsatt för intrångsförsök?

Lite mer än hälften av de svarande visste inte om de hade blivit utsatta för något intrångsförsök. Endast 4 stycken trodde sig att de inte hade blivit utsatta för intrångsförsök.

Fråga 18 - Hur säker anser du att er hemdator är mot Internetrelaterade hot och risker?

Flertalet av de svarande ansåg att de har en okej eller god säkerhet. Något som är värt att notera var att 5 kvinnor, men inga män, ansåg sin säkerhet som mycket god (diagram 6.2.5).

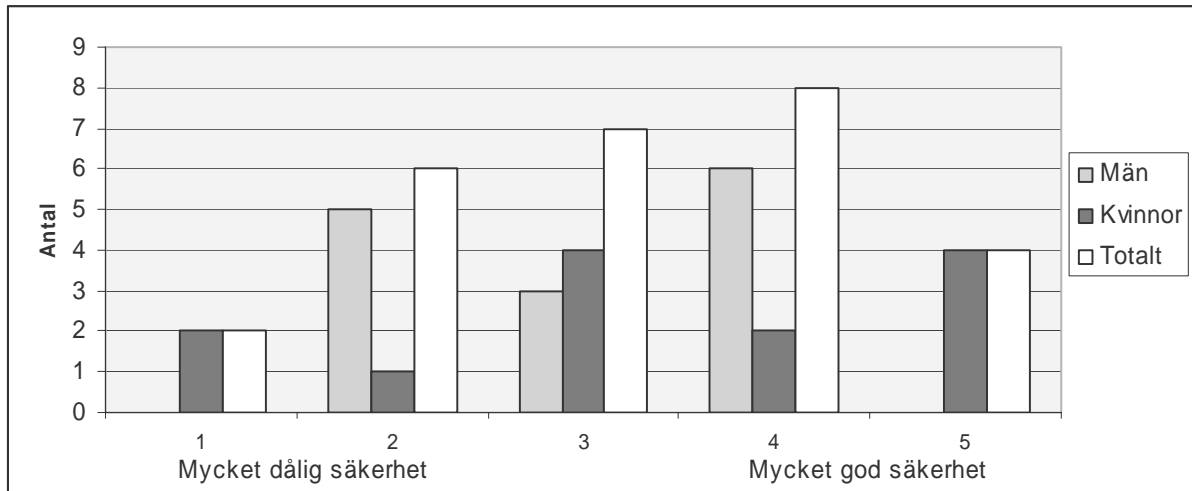


Diagram 6.2.5 (Källa: egen)

7. Resultat - diskussion

Tillgången till hemdatorer har ökat drastiskt de senaste åren (graf 3.1.1). Eftersom tillgången av hemdatorer har ökat har även uppkopplingen mot Internet från hemmen också ökat i samma takt (graf 3.2.1). Dessutom har användningen av olika typer av höghastighetsanslutningar ökat. Detta i sin tur leder till att fler privatpersoner utnyttjar de olika aktiviteter och tjänster som Internet har att erbjuda. Eftersom användandet av Internet har ökat, så har även risken för att bli utsatt för Internetrelaterade hot och risker ökat. Detta har sedan lett till vår problemställning, som i sin tur utmynnat i fem frågeställningar (kap 1.2). Det är dessa fem frågeställningarna som detta kapitel kommer att behandla. Detta kommer vi att göra genom att jämföra vår undersökning mot tidigare undersökningar för att se om det finns tendensskillnader och därmed dra slutsatser om dessa när det är möjligt.

Till vår resultat-diskussion har vi använt, förutom vår egen undersökning, oss av tre tidigare undersökningar: *Privatpersoners användning av datorer och Internet 2003* [SCB, 2004], *Privatpersoners användning av datorer och Internet 2004* [SCB, 2004] och kandidatuppsatsen *Datasäkerheten i hemdatorerna* [Hagman & Meltzer, 2002].

När man jämför olika undersökningar med varandra uppstår det en hel del problem, dessa problem är bland annat; undersökningarna har inte samma syfte, och därför kan liknande frågor uppfattas olika, frågor och svar är inte identiska, stora skillnader på urval, antalet respondenter och könsfördelning. Därför kan vi endast se tendensskillnader mellan vår undersökning och de andra undersökningarna och försöka förklara orsaken till de eventuella tendensskillnaderna.

Undersökning	Urval	Totalt antal respondenter			Totalt antal respondenter med Internetuppkoppling i hemmet		
		Män	Kvinnor	Totalt	Män	Kvinnor	Totalt
H&M, 2002	Ett företag	78	15	93	57	10	67
SCB 2003, 2004	Hela Sverige	3211381	3169008	6380389	2486306	2184423	4670729
SCB 2004, 2004	Hela Sverige	3264110	3213511	6478282	2582712	2504477	5087188
Egen, 2005	Bekvämlighets.	15	16	31	14	14	28

Tabell 7.0.1: Antalet respondenter i absoluta tal. [Källa: (SCB 2003, 2004), (SCB 2004, 2004), (H&M, 2002), (Egen)]

De största problemen med vår undersökning är att vi har väldigt få respondenter samt att vårt urval inte är optimalt för denna typ av undersökning (tabell 7.0.1).

7.1 Ökad uppkopplingstid

Vår frågeställning *ökad uppkopplingstid* (se kap 1.2) går ut på att besvara om Internetanvändandet hos privatpersoner har ökat under de senaste åren. Detta skall vi svara på med hjälp av vår undersökning samt två tidigare gjorda undersökningar, *Privatpersoners användning av datorer och Internet 2003* (SCB, 2004) och kandidatuppsatsen *Datasäkerheten i hemdatorerna* (Hagman & Meltzer, 2002).

Vi kommer att dela in respondenterna i tre grupper. Den första gruppen är de respondenter som inte använder Internet från hemmet. Den andra gruppen är de som använder Internet i

genomsnitt en timme per dygn. Den sista gruppen är de respondenter som använder Internet i genomsnitt mer än en timme per dygn. Anledningen till att vi har delat upp respondenterna i tre grupper såsom: inget, lite och mer, beror på att det skall bli lättare att göra jämförelser mot tidigare undersökningar samt att det kommer att ge ett tydligare resultat.

Den äldsta undersökningen som vi kommer att jämföra mot är *Datasäkerheten i hemdatorerna* (Hagman & Meltzer, 2002). Enligt denna undersökning var det 28 procent av respondenterna som svarade att de inte hade någon tillgång till en Internetanslutning i hemmet, 43 procent använde Internet i genomsnitt mindre än en timme per dygn och slutligen svarade 29 procent att de använde Internet mer än en timme per dygn.

Den andra undersökningen som vi jämför mot är *Privatpersoners användning av datorer och Internet 2003* (SCB, 2004). Enligt denna undersökning var det 27 procent av respondenterna som svarade att de inte hade någon tillgång till en Internetanslutning i hemmet, 55 procent använde Internet i genomsnitt mindre än en timme per dygn och slutligen svarade 18 procent att de använde Internet mer än en timme per dygn.

I vår undersökning kom vi fram till att det var 10 procent av respondenterna som svarade att de inte hade någon tillgång till en Internetanslutning i hemmet, 39 procent använde Internet i genomsnitt mindre än en timme per dygn och slutligen svarade 51 procent att de använde Internet mer än en timme per dygn.

Timmar	Respondenter i procent		
	Egen (2005)	SCB (2004)	H & M (2002)
0	10	27	28
0-1	39	55	43
1-4	32	15	16
4-8	10	2	4
8+	9	1	9

Tabell 7.1.1: Användandet av Internet i procent uppdelat i timmar per dygn. [Källa: (SCB 2003, 2004), (H&M, 2002), (Egen)]

Om man jämför vår undersökning gentemot de andra två undersökningarna ser man tydliga tendenser att Internetanvändandet från hemmen har ökat. Eftersom vi har delat upp respondenterna i tre undersökningsgrupper så kan vi se i vår undersökning att den grupp som inte har någon Internetanslutning i hemmet har minskat gentemot de andra två tidigare undersökningarna. Den gruppen av respondenter som använder Internet i genomsnitt mindre än en timme per dygn har minskat i vår undersökning jämfört med de andra undersökningarna. Slutligen så har vi den gruppen av respondenter som använder Internet mer än en timme per dygn som har ökat i vår undersökning. (Se diagram 7.1.1 och 7.1.2)

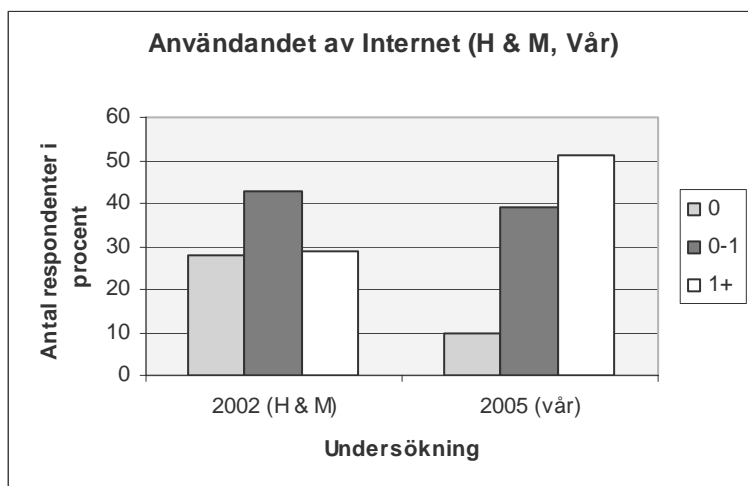


Diagram 7.1.1: Användandet av Internet i procent uppdelat i timmar per dygn. [Källa: (H & M, 2002), (Egen)]

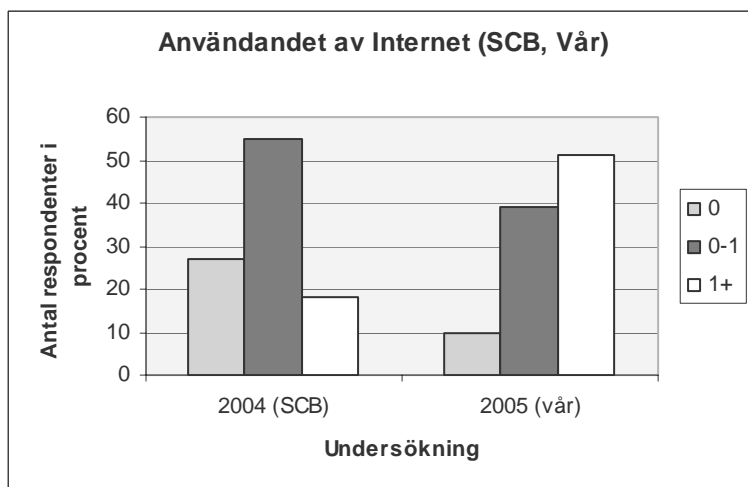


Diagram 7.1.2: Användandet av Internet i procent uppdelat i timmar per dygn. [Källa: (SCB 2003, 2004), (Egen)]

Om man tittar på könsfördelningen i vår undersökning så visar den tydligt att män sitter framför datorn betydligt längre tid än vad kvinnorna gör (se tabell 7.1.2).

Timmar	Respondenter i procent (egen)		
	Män	Kvinnor	Totalt
0	6	12	10
0-1	27	50	39
1-4	27	38	32
4-8	21	0	10
8+	19	0	9

Tabell 7.1.2: Användandet av Internet i procent uppdelat i timmar per dygn och kön. (Källa: Egen)

I vår undersökning tittade vi även på uppkopplingstiden mot Internet. Vi kan inte göra några jämförelser mot de andra undersökningarna på grund av att denna frågeställning saknades på dem. Vi kan enbart konstatera utifrån vår undersökning att hela 54 procent av våra respondenter är uppkopplade mot Internet även under den tiden de inte aktivt använder Internet. (Se diagram 7.1.3)

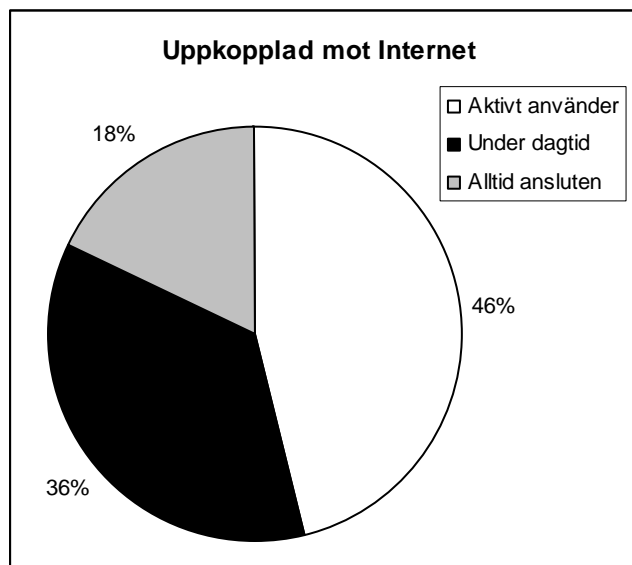


Diagram 7.1.3: Uppkopplad mot Internet. [Källa: Egen]

Enligt ovanstående jämförelser så visar vår undersökning en klar tendens att Internetanvändandet från hemmen har ökat. Denna ökning kan bero på flera olika faktorer. En stor faktor som har påverkat vårt resultat är vårt urval (som förklaras i indelningen av detta kapitel). Andra faktorer som påverkar är bland annat: tillgängligheten till anskaffning av Internet, aktiviteter och tjänster på Internet har ökat, en del av våra respondenter angav att deras Internetanslutning ingick i hyran.

Något som också kan ha bidragit till att fler respondenter har svarat att de använder Internet, men mindre än en timme per dygn, kan bero på svarsalternativen till den relaterade enkätfrågan. Respondenter som hade en Internetanslutning och som inte använde den, kunde inte ange det eftersom alternativet saknades på vår enkät.

7.2 Ökad användning av fast anslutning

Frågeställningen *ökad användning av fast anslutning* (se kap 1.2) går ut på att besvara om fasta anslutningar har ökat i hemmen. Detta skall vi svara på med hjälp av vår undersökning och undersökningarna, *Privatpersoners användning av datorer och Internet 2003* (SCB, 2004) och kandidatuppsatsen *Datasäkerheten i hemdatorerna* (Hagman & Meltzer, 2002).

Vi skriver i vår frågeställning att personer med någon typ av fast anslutning tenderar att vara uppkopplad under än längre tid mot Internet än personer som använder sig av någon typ av uppringd förbindelse. För att bevisa att det verkligen är så kan vi titta på vår egen undersökning. I vår undersökning hade vi sju stycken som hade någon typ av uppringd Internetförbindelse och av dem var det sex respondenter som svarade att de var uppkopplade mot Internet max en timme per dygn. Detta skall jämföras med de respondenter som hade

någon typ av fast Internetanslutning och dessa var i vår undersökning 21 stycken. Dessa 21 respondenterna svarade att de i genomsnitt var uppkopplade en eller flera timmar per dygn. Värt att notera är att 71 procent av de respondenterna med fast anslutning är uppkopplade mot Internet även när de inte aktivt använder det.

För att lättare göra jämförelser mot tidigare undersökningar, så delar vi upp respondenterna i tre grupper. Den första gruppen är de respondenter som inte har någon Internetanslutning i hemmet, vilket medför att de inte kan koppla upp sig mot Internet från hemmet. Den andra gruppen är de respondenter som kopplar upp sig mot Internet med hjälp av någon typ av uppringd förbindelse. Den sista gruppen är de respondenter som har någon typ av fast uppkoppling. Det finns ytterligare en grupp, ”annat”, som vi inte kommer att titta närmare på eftersom den är så pass liten och odefinierbar, denna grupp innehåller bland annat uppkoppling via TV, spelkonsoler, handdatorer mm.

Kandidatuppsatsen från 2002 av Hagman & Meltzer, kom fram till 44 procent av deras respondenter använde sig av någon typ av uppringd Internetförbindelse, 27 procent hade någon typ av fast Internetanslutning i hemmet och 28 procent hade ingen Internetförbindelse.

I *Privatpersoners användning av datorer och Internet 2003* (SCB, 2004), var det 32 procent som hade någon typ av uppringd Internetförbindelse, 32 procent svarade att de hade någon typ av fast Internetanslutning i hemmet och 30 procent hade ingen Internetförbindelse. Om man går lite djupare in på SCB:s undersökning och tittar på könsfördelningen så visar deras undersökning att det var 33 procent av de kvinnliga respondenterna och 31 procent av de manliga som hade någon typ av uppringd Internetförbindelse. Av de kvinnliga respondenterna var det 26 procent och 37 procent av de manliga som svarade att de hade någon typ av fast Internetuppkoppling.

I vår undersökning kom vi fram till att det var 4 procent av de kvinnliga respondenterna jämfört med sju procent av de manliga som hade någon typ av uppringd Internetförbindelse. Detta ger oss totalt 16 procent av våra respondenter som angav att de hade någon typ av uppringd Internetförbindelse. De som angav att de hade någon typ av fast Internetanslutning, var det 62 procent av de kvinnliga respondenterna jämfört med 80 procent av de manliga. Detta ger oss totalt 71 procent av våra respondenter som svarade att de hade någon typ av fast Internetförbindelse. Endast 10 procent av respondenterna hade inte tillgång till Internet från hemmet.

Typ	Respondenter i procent		
	H & M (2002)	SCB (2004)	Vår (2005)
Uppringd	44	32	16
Fast	27	32	71
Annat	1	6	3
Inget	28	30	10

Tabell 7.2.1: Typ av Internetuppkoppling i hemmet.
[Källa: (H&M, 2002), (SCB 2003, 2004), (Egen)]

En tendens som är genomgående i både SCB:s undersökning och i vår undersökning var det att fler kvinnor än män hade en uppringd Internetförbindelse, medan det var vice versa av dem som hade en fast Internetanslutning.

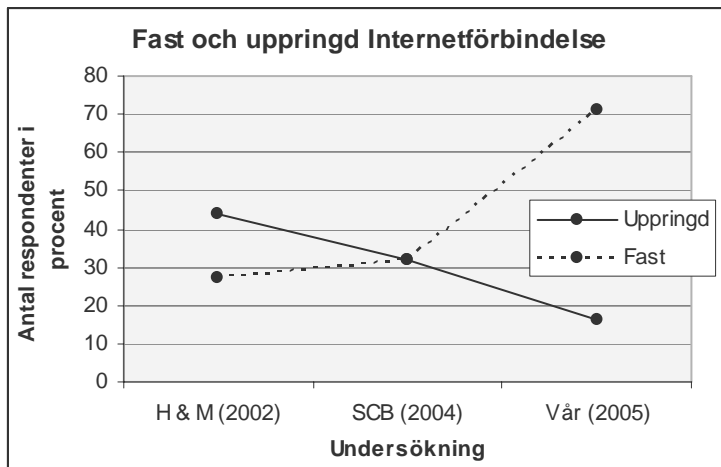


Diagram 7.2.1: Antal respondenter med fast eller uppringd Internetförbindelse. [Källa: (H&M, 2002), (SCB 2003, 2004), (Egen)]

Som vi kan se i diagram 7.2.1 så ser vi tydliga tendenser att användandet av fast Internetuppkoppling har ökat, medan användandet av uppringd förbindelse har minskat. Anledningen till denna drastiska ökning av respondenter, i vår undersökning, som har en fast Internetanslutning är samma faktorer som påverkade ovanstående resultat-diskussion: *Ökad uppkopplingstid* (se kap 7.1).

Något som också kan ha påverkat resultaten, men dock inte speciellt mycket, är vårt sätt att definiera uppringd- och fast- Internetanslutning (se definitionerna som fotnoter i kap 1.2).

7.3 Aktiviteter och tjänster på Internet

Beroende på vilka tjänster och aktiviteter en användare utför kan han eller hon utsätta sig för olika typer av hot och risker. Därför vill vi undersöka vilka *aktiviteter och tjänster* en privatperson använder sig av (frågeställningen från kap 1.2). Utöver en jämförelse av olika aktiviteter och tjänster från tidigare undersökningar, kommer vi att göra en sammanställning av vilka hot och risker som kan tänkas tillhöra respektive aktivitet och tjänst (de som finns med i vår undersökning). De undersökningarna vi valt för att utföra en jämförelse mot vår undersökning är *Privatpersoners användning av datorer och Internet 2004* (SCB, 2004) och *Datasäkerheten i hemdatorerna* (Hagman & Meltzer, 2002). Vi kommer endast att titta på de respondenterna som har en Internetanslutning i hemmet.

De aktiviteter och tjänster som är samma i de tre undersökningarna är: e-maila, chatta, beställa varor/tjänster, banktjänster. Dessa fyra aktiviteter och tjänster kommer vi att jämföra mot varandra i de olika undersökningarna.

Kandidatuppsatsen från 2002 av Hagman & Meltzer, kom fram till följande aktiviteter och tjänster fördelat efter ålder och efter kön:

Aktivitet / tjänst	Ålder					Kön		
	16-24	25-34	35-44	45-54	55-74	Män	Kvinnor	Totalt
Maila	100	100	88	100	100	95	100	96
Chatta	50	38	38	44	36	39	40	39
Beställa varor/tjänster	0	44	42	33	36	37	40	37
Banktjänster	50	63	58	67	64	60	70	61

Tabell 7.3.1: Aktiviteter och tjänster i procent efter ålder och kön. [Källa: Hagman & Meltzer, 2002]

Motsvarande tabell i *Privatpersoners användning av datorer och Internet 2004* (SCB, 2004) ser ut enligt följande:

Aktivitet / tjänst	Ålder					Kön		
	16-24	25-34	35-44	45-54	55-74	Män	Kvinnor	Totalt
Maila	89	91	83	77	69	79	83	81
Chatta	54	24	11	8	11	21	19	20
Beställa varor/tjänster	42	52	46	32	22	40	36	38
Banktjänster	38	71	59	51	40	55	48	51

Tabell 7.3.2: Aktiviteter och tjänster i procent efter ålder och kön. [Källa: *Privatpersoners användning av datorer och Internet 2004*, 2004]

I vår undersökning har vi aktiviteter och tjänster som antingen bara fanns med i den ena eller den andra undersökningen, eller inte fanns med alls. Därför har vi valt att inte göra någon jämförelse med dessa och markerat dessa med en * i tabell 7.3.4.

Aktivitet / tjänst	Ålder					Kön		
	16-24	25-34	35-44	45-54	55-74	Man	Kvinna	Totalt
Maila	100	89	100	83	75	93	86	89
Chatta	75	67	60	17	0	64	29	46
Beställa varor/tjänster	50	89	100	50	50	79	64	71
Banktjänster	50	78	80	83	75	71	79	75
Söka info*	100	100	100	83	50	93	86	89
Ladda ner program/musik*	75	78	60	17	25	79	29	54
Fildelning*	75	67	40	0	25	79	7	43
Spela spel*	50	44	40	33	0	50	21	36
Planlöst surfande*	75	56	40	17	0	57	21	39
Annat*	25	22	0	0	25	29	0	14

Tabell 7.3.4: Aktiviteter och tjänster i procent efter ålder och kön. [Källa: Egen]

Genom att jämföra de tre undersökningarna kan man hitta liknande eller olika tendenser för de olika aktiviteterna/tjänsterna.

E-maila

Tendensen i de tre undersökningarna är att det är mycket vanligt i alla åldrar att e-maila, men sjunker en aning i de äldre ålderskategorierna. I vår undersökning är det en liten övervikt för männen mot kvinnorna, vilket är det samma i SCB:s undersökning.

Chatta

Tendensen i de tre undersökningarna när det gäller att chatta är vanligast i de yngre åldersgrupperna för att sedan sjunka i de äldre åldersgrupperna. I vår undersökning hade vi en ganska stor skillnad mellan de olika könen jämfört med de två andra undersökningarna.

Beställa varor/tjänster

De ålderskategorierna som mest beställer varor och tjänster på Internet är 25-34 och 35-44, vilket gäller för de tre undersökningarna. Noterbart är det att i vår undersökning var denna aktivitet/tjänst mycket vanligare än i de övriga två undersökningarna.

Banktjänster

De ålderskategorierna som minst använder sig av banktjänster på Internet är den lägsta 16-24 samt den äldsta 55-74, vilket gäller för de tre undersökningarna. Det är inte någon större skillnad när det gäller könsfördelningen av de respondenter som använder sig av banktjänster på Internet.

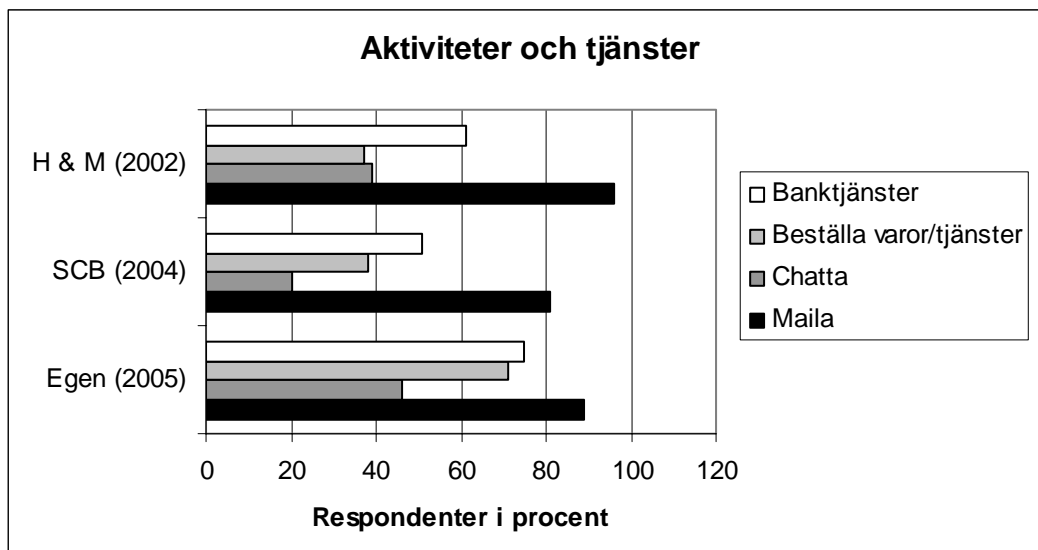


Diagram 7.3.1: Aktiviteter och tjänster i procent. [Källa: (H & M, 2002), (SCB 2004, 2004), (Egen)]

Att utföra olika typer av aktiviteter och tjänster på Internet kan medföra olika typer av hot och risker. Om vi tittar på de aktiviteter och tjänster som vi har presenterat i detta delkapitel, kan vi med hjälp av vårt säkerhetskapitel (se kap 4) associera vilka hot och risker som tillhör respektive aktiviteter/tjänster. De flesta hot och riskerna som vi skriver om här nedan kan man undvika med hjälp av olika typer av säkerhetsprogram/rutiner, men dessa tar vi inte upp här. Det skall också tilläggas att det finns en mängd fler hot och risker som vi inte tar upp.

E-maila

Spam är det största problemet när det gäller e-mail som de flesta e-mailanvändare mer eller mindre har fått erfara. Förutom Spam finns det många andra hot och risker en e-mailanvändare kan utsättas för, dessa är olika typer av Spyware och i stort sätt alla typer av skadlig kod. Oftast när det gäller skadlig kod så måste användaren själv exekvera den skadliga koden för att drabbas av dessa hot och risker. Ytterligare ett problem med e-mail är att man aldrig kan vara säker på om någon annan läser av ens post.

Chatta

Detta är nog den aktivitet som är minst utsatt för hot och risker, men dock inte helt utan problem. Det vanligaste problemet är att man kan utsättas för diverse Spyware samt att man aldrig är helt säker på att det man säger i en chatt är konfidentiellt, det finns alltid en risk att det är någon som "tjuvlyssnar".

Beställa varor/tjänster

Att beställa varor/tjänster över Internet innebär en del säkerhetsrisker. En risk en användare kan råka ut för är att en såkallad Cracker försöker att stjäla användarens lösenord och kortinformation. En annan risk är att användaren inte har någon inblick över hur företaget behandlar den information användaren lämnar ut. Denna information kan säljas till ett företag som har specialiserat sig att bygga databaser där all information om användarens köpvanor finns lagrat. Även Spyware som finns på användarens dator kan samla information om användaren.

Banktjänster

Det största hotet mot de olika typer av banktjänster som finns på Internet är de såkallat Crackers. Dessa Crackers använder all sin kunskap för att ta sig in i de olika banksystemen för att antingen stjäla eller ställa till förtret.

Enligt vår undersökning så har vi större andel personer procentuellt i aktiviteterna/tjänsterna, banktjänster, chatta och beställa varor/tjänster, medan e-maila är procentuellt ungefär samma som de tidigare undersökningarna (se diagram 7.3.1). Noterbart är att förhållandena mellan de olika aktiviteterna/tjänsterna någorlunda lika mot de andra undersökningarna. Tendensökningen i vår undersökning kan bero på flera olika faktorer. En stor faktor som har påverkat resultatet är vårt urval (som förklaras i indelningen av detta kapitel). Andra faktorer som påverkar är bland annat: tillgängligheten av Internet, enklare och fler tjänster/aktiviteter på Internet och att fler och fler tjänster/aktiviteter underlättas/krävs att man utför dem på Internet.

7.4 Säkerhetsmedvetande hos privatpersoner

När en privatperson är uppkopplad mot Internet kan han eller hon utsättas för olika hot och risker. Därför gäller det för användaren att försöka införskaffa sig kunskap och kännedom om dessa. Den kunskapen och kännedomen som en användare besitter har vi i denna frågeställning kallat för säkerhetsmedvetande.

För att få reda på våra respondenters säkerhetsmedvetande har vi ställt några grundläggande frågor som handlar om erfarenhet, läsvanor, hot kännedom, attacker mot hemdatorn samt hur säkra de själva anser sin hemdator är mot Internetrelaterade hot och risker. Vi kommer även att redovisa vad våra respondenter vidtar för säkerhetsåtgärder, om de utför några, när de laddar hem ett program eller en musikfil. Resultaten ska sedan jämföras mot kandidatuppsatsen *Datasäkerheten i hemdatorerna* [Hagman & Meltzer, 2002], i den mån det går, för att se om det finns några tendensförändringar i säkerhetsmedvetandet hos privatpersoner. De respondenter som ingår i undersökningarna i detta delkapitel har en Internetanslutning i hemmet.

Datorerfarenhet

En av frågorna på vår enkät frågade respondenten om hur många års datorvana han/hon har. Den åldersgrupp som har mest datorerfarenhet är de som är 25-34 år gamla och de står för 25 procent av våra respondenter. Om man tittar på könsfördelningen så är männen överrepresenterade i den högsta gruppen.

År	Ålder (antal)					Kön (%)		Totalt (%)
	16-24	25-34	35-44	45-54	55-74	Män	Kvinnor	
0-1	0	0	0	1	0	0	7	4
1-3	1	0	0	2	2	14	21	18
3-6	0	2	3	1	0	14	29	21
6+	3	7	2	2	2	72	43	57

Tabell 7.4.1: Datorerfarenhet i antal respondenter och i procent. [Källa: Egen]

År	Respondenter (%)
0-1	0
1-4	40
4-7	29
7+	31

Tabell 7.4.2: Datorerfarenhet i antal respondenter i procent. [Källa: Hagman & Meltzer, 2002]

Om vi tittat på H&M:s undersökning, så visar den att fördelningen av deras respondenter när det gäller datorerfarenhet är ganska lika, med en liten övervikt i kategorin 1-4 år. Detta ger oss att datorerfarenheten har ökat med vår undersökning jämfört med H&M:s undersökning. Denna ökning är självklar, eftersom både datorinnehav och Internetanslutning i hemmen har ökat sedan deras undersökning (se kap 3).

Läsvanor

När det gäller respondenternas läsvanor när det gäller någon teknisk tidskrift så har det sänkts markant om man jämför H&M:s undersökning mot vår. Den drastiska förändringen kan bero på många faktorer. En bidragande faktor som vi tror kan påverka är att folk föredrar att inhämta denna information gratis och lättare på Internet, än att fysiskt köpa en teknisk tidskrift.

Svarsalternativ	Undersökning i procent	
	H & M (2002)	Egen (2005)
Ja	46	7
Nej	54	93

Tabell 7.4.3: Läser regelbundet någon teknisktidskrift. [Källa: (Hagman & Meltzer, 2002), (Egen)]

Säkerhetsrisker

För att undersöka respondenternas kännedom om olika hot och risker ställde vi en fråga på enkäten om detta. Definitionen av själva frågan på vår enkät skiljer sig mot motsvarande fråga som H&M ställde på sin, och därför kan de inte jämföras direkt. Skillnaden mellan de två undersökningarna är det att vi ställde frågan om de kunde förklara vad de olika termernas innebörd, medan H&M frågade om de bara kände till/hört talas om termerna. Därför kan vi dra slutsatsen att kännedomen av de olika hot- och risktermerna har ökat sedan H&M gjorde sin undersökning.

Hot/risk	Undersökning			
	Egen (2005)			H & M (2002)
	Män (%)	Kvinnor (%)	Totalt (%)	Totalt (%)
Maskar	64	21	43	42
Trojaner	86	14	50	48
Bakdörr	57	14	36	31
Portskanning	57	0	29	13
Spyware*	64	7	36	-
Netbus*	50	0	25	-

Tabell 7.4.5: Kännedom/hört talas om hot- och risktermer. [Källa: (Hagman & Meltzer, 2002), (Egen)]

Vidare kan man urskilja i vår undersökning att männens kännedom av de olika hot- och risktermerna var betydligt större än kvinnornas. Denna skillnad antar vi att det beror på att männen använder och utnyttjar datorn betydligt mer än vad kvinnorna gör.

Virusangrepp

Totalt sett är det flest respondenter i båda undersökningarna som säger sig ha blivit utsatt för virusangrepp. Det är fler respondenter i vår undersökning som har blivit utsatt för virusangrepp än H&M:s undersökning och av respondenterna i vår undersökning så är det merparten män. De respondenter som säger sig att inte blivit utsatt för något virusangrepp har minskat i vår undersökning jämfört med H&M:s och det är fler kvinnor än män som har angett detta alternativet i vår undersökning. Om man tittar på de respondenter som inte vet om de har blivit utsatt för något virusangrepp har ökat jämfört med H&M:s undersökning.

Skillnaderna mellan de båda undersökningarna kan bero på att det blir allt mer vanligare med virus samt att medvetenheten om virushoten har ökat.

Svarsalternativ	Undersökning			
	Egen (2005)			H&M (2002)
	Män (%)	Kvinnor (%)	Totalt (%)	Totalt (%)
Ja	79	43	61	46
Nej	14	21	18	39
Vet ej	7	36	21	15

Tabell 7.4.6: Utsatt för virusangrepp i procent. [Källa: (Hagman & Meltzer, 2002), (Egen)]

Intrångsförsök

I vår undersökning är det procentuellt fler respondenter som säger att de har utsatts för intrångsförsök än om man jämför med H&M:s undersökning. Tittar man på könsfördelningen i vår undersökning så är det stor övervikt för männen där 43 procent säger sig ha blivit utsatt för någon typ av intrångsförsök jämfört med bara sju procent av kvinnorna.

Jämför man vidare mellan undersökningarna kan man urskilja att de respondenter som svarade att de aldrig blivit utsatt för någon typ av intrångsförsök skiljer sig mycket i de båda undersökningarna. I vår undersökning var det 14 procent som angav det svarsalternativet medan det var 42 procent i H&M:s undersökning. Vidare kan man se i vår undersökning att det är många fler kvinnor än män som angav att de aldrig blivit utsatta för intrångsförsök.

När det gäller svarsalternativet vet ej var det hela 61 procent som svarade det i vår undersökning medan motsvarande svarsalternativ hade 46 procent i H&M:s undersökning. Tittar man på könsfördelningen i vår undersökning var det hälften av männen som angav detta svarsalternativ och hela 71 procent av kvinnorna.

Svarsalternativ	Undersökning			
	Egen (2005)			H&M (2002)
	Män (%)	Kvinnor (%)	Totalt (%)	Totalt (%)
Ja	43	7	25	12
Nej	7	22	14	42
Vet ej	50	71	61	46

Tabell 7.4.7: Utsatt för intrångsförsök i procent. [Källa: (Hagman & Meltzer, 2002), (Egen)]

De stora skillnaderna mellan de olika undersökningarna kan antas bero på att det är allt vanligare med intrångsförsök samt att kunskapen att skydda sig och att upptäcka intrångsförsök har ökat.

Vid nedladdning

Vi kommer inte att göra någon jämförelse mot någon tidigare undersökning när det gäller nerladdning av program och musik från Internet eftersom vi inte har lyckats att hitta någon liknande undersökning som går att jämföra mot.

Det vanligaste alternativet våra respondenter svarade var att de kontrollerar att virusprogrammet är på innan de kör nerladdad program eller musik. Detta är lite svårt att veta hur våra respondenter tolkade svarsalternativet, men vi antar att de egentligen inte kollade efter om antivirusprogrammet var på eller inte innan de körde programmet eller musikfilen. Detta är på grund av att de flesta antivirusprogram startas automatiskt med operativsystemet och ligger sen i bakgrunden för att skanna datorns internminne kontinuerligt. Noterbart är att det var betydligt fler män än kvinnor som svarade detta alternativet.

Det näst vanligaste alternativet var att våra respondenter svarade att de inte laddade hem något program eller musik från Internet. Skillnaden mellan könen är också här mycket stor, med en stark övervikt för kvinnor.

Åtgärd innan körning av program- eller musikfil i procent			
Svarsalternativ	Män	Kvinnor	Totalt
Kör genast	29	14	21
Kontrollerar att antivirus är på och sen kör	50	14	32
Skannar filen och sen kör	0	22	11
Laddar inte hem	7	43	25
Annat	14	7	11

Tabell 7.4.8: Åtgärd innan körning av program- eller musik-fil. (Källa: Egen)

Egen säkerhet

När det gäller hur våra respondenter anser hur säkert deras hemdator är mot Internetrelaterade hot och risker så skall vi försöka göra en jämförelse mot en liknande undersökning i Hagmans och Meltzers undersökning. Själva jämförelsen är lite problematisk på grund av att vi använder oss av en fem gradig skala, medan H&M använder sig av en fyrgradig skala. Men vi antar att det går att jämföra de båda ytterligheterna med varandra på grund av att skalorna i de olika undersökningarna skiljer sig endast med en grad. Vi kommer även att göra en mindre korrekt jämförelse av mellangraderna (de graderna som ligger mellan ytterligheterna) genom att summera dem, för att få en ungefärlig jämförelse.

I vår undersökning var det sju procent av respondenterna som ansåg att sin hemdator var mycket dålig mot Internetrelaterade hot och risker. Motsvarande siffra i H&M:s undersökning var 25 procent. De respondenter som ansåg att deras hemdator var mycket säker var 15 procent i vår undersökning, medan bara fyra procent i H&M:s undersökning. Om man jämför

graderna mellan ytterligheterna så får vår undersökning 78 procent jämfört med 71 procent i H&M:s undersökning. Detta ger oss att tendensen när det gäller säkerheten mot Internetrelaterade hot och risker har ökat sedan H&M gjorde sin undersökning.

Datorsäkerhet (egen)			
Säkerhetsgrad	Män (%)	Kvinnor (%)	Totalt (%)
1 (Mycket dåligt)	0	15	7
2	36	8	22
3	21	31	26
4	43	15	30
5 (Mycket bra)	0	31	15

Tabell 7.4.9: Datorsäkerhet. (Källa: Egen)

Datorsäkerhet (H&M)	
Säkerhetsgrad	Totalt (%)
1 (Mycket dåligt)	25
2	40
3	31
4 (Mycket bra)	4

Tabell 7.4.10: Datorsäkerhet (Källa: H&M, 2002)

En intressant aspekt är att många av våra kvinnliga respondenter svarade att de hade mycket dålig eller mycket bra säkerhet mot Internetrelaterade hot och risker, medan inga av männen angav dessa två ytterligheterna. Av vår egen erfarenhet är det väldigt sällan att en person med stor kunskap om säkerhet säger att han/hon själv har mycket bra säkerhet. Detta är på grund av att personer som är väl medvetna om olika hot och risker är även medvetna om att det är mycket svårt att skydda sig mot allt.

Sammanfattningsvis kan man se en del tendensskillnader i detta delkapitel. Datorerfarenheten och kunskaper om Internetrelaterade hot och risker har båda ökat. Men att bli drabbad av virus eller intrång har också ökat, fast kunskaperna om dessa är högre. Detta kan förklaras genom att det finns betydligt fler säkerhetshot i dag kombinerat med att man är mer medveten om de olika hot och riskerna vilket i sin tur leder till att man lättare upptäcker dem.

Skillnaden mellan de båda könen i vår undersökning är markant. Det är vanligare att kvinnorna har svarat att de inte har blivit utsatt för virus eller intrångsförsök samt alternativet vet ej. Vi tror att de som har svarat att de inte har blivit utsatta för virus eller intrångsförsök inte har kunskapen att upptäcka dessa, eftersom det är svårt att säga att man aldrig blivit utsatt för virus eller intrångsförsök. Vidare så var kunskapen lägre hos kvinnorna när det gäller kännedomen om de olika hot och riskerna.

En faktor som kan ha påverkat våra resultat i detta delkapitel är vårt urval (som förklaras i indelningen av detta kapitel). Ytterligare faktorer som kan ha påverkat resultaten är själva utformningen av våra enkätfrågor. De enkätfrågor som handlar om att våra respondenter har blivit utsatta för virusangrepp och intrångsförsök har vi angivit svarsalternativet nej vilket det i stort sett är omöjligt att svara. Att man inte kan svara nej på de frågorna beror på att det är svårt att veta om man har utsatts för virus (elakartad kod) eller intrångsförsök. Vidare så är själva definitionen om vad virusangrepp är lite tvetydlig i vår fråga. Respondenterna har kanske inte tänkt på att virusbegreppet i frågan även innehåller Maskar, Trojaner, Spyware och andra elakartade koder vilket var en miss från vår sida.

7.5 Säkerhetsåtgärder hos privatpersoner

Det finns en mängd Internetrelaterade hot och risker, som vi har beskrivit i vårt arbete, men det finns även olika sätt att skydda sig mot dessa (se kap 5). Därför kommer detta delkapitel handla om jämförelser mellan vår undersökning och *Datasäkerheten i hemdatorerna*

(Hagman & Meltzer, 2002) för att se om vi kan hitta några tendensförändringar i vilka säkerhetsåtgärder privatpersoner använder sig av. Vi hade hoppats att kunna göra jämförelser mot SCB:s olika undersökningar också, men det visade sig att de hade för lite information om detta ämne för att kunna göra en ordentlig jämförelse. Vi kommer endast att titta på de respondenterna som har en Internetanslutning i hemmet.

De båda undersökningarna visar klart och tydligt att tre typer av säkerhetsåtgärder är mest använda och dessa är; brandvägg, antivirusprogram och säkerhetsuppdateringar av operativsystemet. Tendens för dessa tre säkerhetsåtgärder är att den har ökat i vår undersökning jämfört med H&M:s undersökning. Den största tendensökningen står användandet av brandvägg med 33 procent, efter det så har säkerhetsuppdateringar av operativsystem ökat med 26 procent. Användandet av antivirusprogram har inte tendensförändring blivit lika stor, men dock en ökning med åtta procent. Tendenskillanden när det gäller de privatpersoner som inte använder sig av någon säkerhetsåtgärd har minskat med åtta procent. I stort sätt så har användandet av säkerhetsåtgärder ökat och detta beror på att Internetrelaterade hot och risker också ökat samt att kunskapen och medvetenheten om dessa har ökat (se kap 7.4)

Säkerhetsåtgärder hos privatpersoner						
Säkerhetsåtgärd	Egen (2005)			H&M (2002)		
	Män (%)	Kvinnor (%)	Totalt (%)	Män (%)	Kvinnor (%)	Totalt (%)
Brandvägg	50	64	57	21	40	24
Antivirusprogram	79	71	75	68	60	67
Filterprogram	0	0	0	7	0	4
Krypteringsprogram	7	0	4	5	0	4
Säkerhetsuppdat.	64	36	50	26	10	24
Användarpolicy	21	7	14	9	0	7
Annat	14	0	7	0	0	0
Inget skydd	0	7	4	12	10	12
Vet ej	14	14	14	12	30	15

Tabell 7.5.1: Säkerhetsåtgärder hos privatpersoner i procent. [Källa: (Hagman & Meltzer, 2002), (Egen)]

Om man tittar på könsfördelningen på de tre vanligaste säkerhetsåtgärderna så visar båda undersökningarna samma mönster när det gäller fördelningen mellan könen. Att det var fler kvinnor än män som använde sig av någon typ av brandvägg i båda undersökningarna tror vi kan förklaras med att kvinnorna inte i lika stor utsträckning som män utför aktiviteter och tjänster där en brandvägg kan ställa till med problem (se tabell 7.3.4). Det är fler män än kvinnor i båda undersökningarna som använder sig av ett antivirusprogram. Detta kan kanske förklaras genom att män utför fler aktiviteter och tjänster (nerladdning, fildelning, spela spel) och därigenom är mer beroende av att ha ett antivirusprogram. Även när det gäller säkerhetsuppdateringar av operativsystemet är det fler män än kvinnor som gör detta. Anledningen varför man uppdaterar sitt operativsystem är på grund av att det ständigt uppkommer säkerhetsbrister och man måste därför förhindra dessa genom att uppdatera operativsystemet. Att det är fler män än kvinnor som gör detta kan bero på kunskapen om Internetrelaterade hot och risker (se kap 7.4).

Precis som med resultaten i hela vår resultat-diskussion kan vi bara urskilja tendenser på grund av vårt urval (som förklaras i indelningen av detta kapitel). Ytterligare ett problem i detta delkapitel var att könsfördelningen i H&M:s undersökning endast bestod av 15 procent kvinnliga respondenter.

8 Slutsats

Eftersom vår undersökning inte blev så bred som vi hade hoppats på och att vårt urval blev väldigt begränsat innebär detta att vi endast har kunnat se tendensskillnader vid jämförelser mellan de olika undersökningarna. Detta i sin tur ger oss att vi endast kan påpeka tendenser när vi skall svara på vår problemställning som är: ”Hur privatpersoners Internetanvändning ser ut samt deras medvetenhet om skydd, hot och risker.”

Privatpersoners Internetanvändning

För att kunna svara på privatpersoners Internetanvändning, som är en del av vår problemställning svarade vi på följande frågeställningar; *ökad uppkopplingstid, ökad användning av någon typ av fast Internetanslutning och aktiviteter och tjänster på Internet.*

Utifrån vår resultat-diskussion kom vi fram till en tydlig tendens att uppkopplingstiden mot Internet har ökat samt att någon typ av fast Internetanslutning blir allt vanligare. Vidare visade vår undersökning att användandet av de flesta aktiviteter och tjänster har ökat, medan att e-maila är ungefär det samma som tidigare undersökningar.

Privatpersoners säkerhetsmedvetenhet

Nästa del i vår problemställning är att ta reda på om privatpersoners medvetenhet om olika Internetrelaterade hot och risker har blivit bättre. För att kunna svara på denna del av problemställningen använde vi frågeställningen *säkerhetsmedvetande hos privatpersoner.*

Det som kom fram i vår resultat-diskussion var att både kunskapen och medvetenheten om Internetrelaterade hot och risker har ökat. Även om kunskapen och medvetenheten har blivit bättre finns det tendenser på att allt fler blir drabbade av virus eller intrångsförsök.

Säkerhetsåtgärder hos privatpersoner

Den sista delen av vår problemställning tar upp vad privatpersoner gör för att skydda sig mot Internetrelaterade hot och risker. Till vår hjälp använde vi oss av frågeställningen *säkerhetsåtgärder hos privatpersoner.*

Det som vi kom fram till i vår resultat-diskussion var att det fanns en tydlig tendens på att fler skyddar sig mot Internetrelaterade hot och risker än tidigare år.

9 Vidare forskning

Som vi har skrivit i vårt inledande kapitel (kap 1.1) ökar Internetanvändandet, vilket även visas i kapitel 3 och i vår sammanfattning (kap 8). Denna ökning av Internetanvändandet kommer förmodligen inte att minska i den närmsta framtiden eftersom vi blir allt mer beroendet av Internet för att utföra dagliga aktiviteter och tjänster. Självklart kommer ökningen av Internetanvändandet att planas ut, men kommer att göra detta på en högre nivå än nu. Därför kommer det att vara intressant att man kontinuerligt forskar vidare inom detta område för att se hur Internetanvändandet och dess konsekvenser förändras, inte bara för privatpersoner utan för hela samhället.

10 Källförteckning

Böcker

Andersson, B-E.(2001). *Som man frågar får man svar*. Göteborg: Elanders Digitaltryck

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

Bryman, A. (2004). *Samhällsvetenskapliga metoder*. Slovenien: Korotan Ljubljana

Panko, R. (2003). *Business Data Networks and Telecommunications*.

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

Pfeeger, C & Pfeeger S. (2003) *Security in Computing*. USA: Pearson Education

Stallings, W. (2000). *Network Security Essentials*. USA: Prentice-Hall

Rapporter

Hagman, M & Meltzer, M (2002). *Datorsäkerheten i hemdatorerna*. Lunds Universitet Institutionen för Informatik.

Webbdokument

Anderberg, S. (2004). *Primär- & sekundärkälla*.

URL:http://www.infosokaren.se/infokallor_primarsek.asp 2005-09-29

Axelsson, P (2001) *UpUnet - S guide till Internet*. Uppsala Universitet

URL:<http://www.student.uu.se/upunets/guide/index.phtml> 2005-09-29

CyberPatrol

URL:<http://www.cyberpatrol.com/> 2005-09-29

F-Secure. (1999). *F-Secure virusinformation*.

URL:

<http://www.f-secure.se/virus/virusinfo.asp?Namn=Netbus> 2005-09-29

F-Secure. (2003). *Trojan (generisk beskrivning)*

URL:<http://www.f-secure.se/virus/virusinfo.asp?Namn=Trojan> 2005-09-29

Harvey, Brian. *What is a hacker?*

URL:<http://www.cs.berkeley.edu/~bh/hacker.html> 2005-09-29

Incabus Systems (2004) *Anti-spionprogram*

URL: <http://www.incabus.com/se/info/antispypware.html> 2005-09-29

Indiana University

URL: <http://kb.iu.edu/data/agwt.html> 2005-09-29

Microsoft. (2005). *Introduktion till virus maskar och trojanska hästar*.

URL:<http://www.microsoft.com/sverige/security/latest/articles/2004/virusintroduktion.asp>

2005-09-29

Microsoft, (2005). *Spam*

URL: <http://www.microsoft.com/sverige/security/threats/spam.asp> 2005-09-29

Microsoft, (2005). *Undvik spionprogram*

URL: <http://www.microsoft.com/sverige/security/threats/spy.asp> 2005-09-29

Microsoft. (2005). *Vad är en trojansk häst?*

URL: <http://www.microsoft.com/sverige/security/threats/trojan.asp> 2005-09-29

Nationalencyklopedin, (2005)

URL: <http://www.ne.se> 2005-09-29

Netnanny

URL: <http://www.netnanny.net/> 2005-09-29

Observatoriet för informationssäkerhet. (2000). *Säkerhet på Internet – Datavirus och blockering av tjänster*

URL: http://www.itkommissionen.se/dynamaster/file_archive/020124/4edc090cf3a63a1b6b701a9baa803122/23_2000%20S%e4kerhet%20p%e5%20Internet%20-%20Datavirus%20och%20blockering%20av%20tj%e4nster.pdf 2005-09-29

Post och Telestyrelsen. (2005). *Spionprogram och andra närliggande företeelser.*

URL: http://www.pts.se/Archive/Documents/SE/Spionprogram_sve.pdf 2005-09-29

Post och Telestyrelsen. (2005). *Surfa säkrare. Goda råd om säkerhet på Internet.*

URL: http://www.pts.se/Archive/Documents/SE/Surfa-sakrare_last.pdf 2005-09-29

ROMAB. (2005). *Nätverkssäkerhet. Grunder fortsättning.*

URL: <http://www.isk.kth.se/kursinfo/6b3008/files/F2.pdf> 2005-09-29

Secure-IT (2005). *Vad är fientlig kod?*

URL: <http://www.secure-it.se/index.htm> 2005-09-29

Statistiska Centralbyrån. (2004). *Privatpersoners användning av datorer och Internet 2003.*

URL: http://www.scb.se/statistik/IT/IT0102/2003M00/IT0102_2003M00_BR_TKFT0401.pdf 2005-09-29

Statistiska Centralbyrån. (2004). *Privatpersoners användning av datorer och Internet 2004.*

URL: http://www.scb.se/statistik/_publikationer/IT0102_2004A01_BR_TKFT0404.pdf 2005-09-29

11 Bilagor

11.1 Enkät

Enkätundersökning

Hej!

Vi är två studenter vid namn Jesper Rodriguez och Linus Pålhorstorp som studerar Informatik på Lunds Universitet. Vi håller på att skriva vår kandidatuppsats om datorsäkerhet i hemdatorerna relaterat till Internet uppkoppling. Syftet med denna enkät är att få en uppfattning om och hur man skyddar sina hemdatorer, samt vilka Internettjänster de använder och vilka kunskap de besitter inom området.

All information som du lämnar på denna enkätundersökning kommer att vara helt anonymt och kommer inte att användas till något annat syfte än till underlag för vår undersökning.

Vi kommer att använda oss av två olika val symboler:

– Endast ett alternativ får kryssas i.

– Flera alternativ får kryssas i.

Tack på förhand att ni svarar på våra frågor.

1. Kön?

Man Kvinna

2. Hur gammal är du?

16-24 25-34 35-44 45-54 55-74

3. Utbildningsnivå (Ange endast högsta avslutande nivå)?

Grundskola Gymnasial Eftergymnasial

4. Har du tillgång till en dator med Internetuppkoppling i hemmet?

Ja Nej Vet ej

OBS! Svara endast på efterföljande frågor om ni har svarat "ja" på frågan nummer 4.

5. Hur betalar du för er Internetuppkoppling?

Betalningen beror på uppkopplingstiden

Betalningen beror på hur mycket jag laddar ner

Betalar en fast avgift som inte är beroende på hur mycket jag nyttjar Internet

Vet ej

6. Vilken typ av uppkoppling har du i hemmet?

- Modem (uppringd förbindelse via telefonnätet)
- ISDN
- ADSL
- Kabelmodem
- Fast uppkoppling (exempelvis LAN)
- Annat: _____

7. Vilken är den främsta orsaken till ditt val av uppkoppling i hemmet?

- Ekonomiska skäl
- Bättre säkerhet
- Går snabbare
- Stabilare och enklare att koppla upp sig
- Annat: _____

8. Hur länge är du aktivt uppkopplade mot Internet under ett genomsnittligt dygn? (Aktivt menas hur många timmar ni sitter vid datorn och nyttjar Internet)

- 0-1 1-4 4-8 8-

9. Hur länge brukar er hemdator vara uppkopplad mot Internet?

- Bara under den tiden som jag eller någon annan aktivt använder datorn
- Datorn är oftast uppkopplad mot Internet under dagtid
- Datorn är alltid uppkopplad mot Internet

10. Hur många års erfarenhet med datorer har du? (Behöver inte enbart vara hemdatorer)

- 0-1 1-3 3-6 6-

11. Vilken/vilka aktiviteter och tjänster använder du på Internet?

- Maila
- Chatta
- Beställa varor/tjänster
- Banktjänster
- Söka information
- Ladda ner program/musik från hemsidor
- Fildelning (Exempelvis via FTP, Direct Connect, Bittorrent mm.)
- Spela spel
- Planlöst surfande
- Annat: _____

11.2 Enkätamanställning

Fråga 1

	Kön (antal)		
	Män	Kvinnor	Totalt
Antal	15	16	31

Fråga 2

	Ålder (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Antal	3	2	5	4	3	2	0	6	4	2

	Kön (antal)		
	Män	Kvinnor	Totalt
Antal	15	16	31

Fråga 3

	Utbildning (antal)									
	16-24		25-34		35-44		45-54		55-74	
Alt.	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Grund	1	0	0	0	0	0	0	1	0	1
Gym	0	1	2	0	1	1	0	1	1	1
Egym	2	1	3	4	2	1	0	4	3	0

Alternativ	Kön (antal)		
	Män	Kvinnor	Totalt
Grund	1	2	3
Gym	4	4	8
Egym	10	10	20

Fråga 4

	Tillgång till Internetuppkopplad hemdator (antal)									
	16-24		25-34		35-44		45-54		55-74	
Alternativ	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Ja	3	1	5	4	3	2	0	6	3	1
Nej	0	1	0	0	0	0	0	0	1	1
Vet ej	0	0	0	0	0	0	0	0	0	0

Alternativ	Kön (antal)		
	Män	Kvinnor	Totalt
Ja	14	14	28
Nej	1	2	3
Vet ej	0	0	0

Fråga 5

Alternativ	Betaling för Internetuppkoppling (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Uppkopplings tid	0	0	0	2	1	1	0	0	0	1
Nedladdning	0	0	0	0	0	0	0	0	0	0
Fast	3	1	5	2	2	1	0	6	3	0
Vet ej	0	0	0	0	0	0	0	0	0	0

Alternativ	Kön (antal)		
	Män	Kvinnor	Totalt
Uppkopplings tid	1	4	5
Nedladdning	0	0	0
Fast	13	10	23
Vet ej	0	0	0

Fråga 6

Typ	Uppkopplings typ (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Modem	0	0	0	2	1	1	0	0	0	1
ISDN	0	0	0	0	0	0	0	0	0	0
ADSL	0	1	2	1	0	1	0	6	3	0
Kabel	1	0	0	0	1	0	0	0	0	0
Fast	2	0	2	1	1	0	0	0	0	0
Annat	0	0	1	0	0	0	0	0	0	0

Typ	Kön (antal)		
	Män	Kvinnor	Totalt
Modem	1	4	5
ISDN	0	0	0
ADSL	5	9	14
Kabel	2	0	2
Fast	5	1	6
Annat	1	0	1

Fråga 7

Alternativ	Främsta orsak till uppkopplings typ (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Ekonomiskt	1	0	0	3	2	1	0	0	0	0
Säkrare	0	0	0	0	0	0	0	0	0	0
Går snabbare	1	1	0	0	0	0	0	1	1	0
Enklare	0	0	0	0	0	0	0	2	2	1
Annat	1	0	5	1	1	1	0	2	0	0

(en kvinna ej svarat i åldern 45-54)

Alternativ	Kön (antal)		
	Män	Kvinnor	Totalt
Ekonomiskt	3	4	7
Säkrare	0	0	0
Går snabbare	2	2	4
Enklare	2	3	5
Annat	7	4	11

Fråga 8

Timmar	Uppkopplingstid ett genomsnittligt dygn (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
0-1	0	1	1	3	1	2	0	1	2	1
1-4	2	0	1	1	0	0	0	5	1	0
4-8	1	0	1	0	1	0	0	0	0	0
8-	0	0	2	0	1	0	0	0	0	0

Timmar	Kön (antal)		
	Män	Kvinnor	Totalt
0-1	4	8	12
1-4	4	6	10
4-8	3	0	3
8-	3	0	3

Fråga 9

Alternativ	Uppkopplad mot Internet (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Aktivt använder	0	0	1	3	2	1	0	3	2	1
Under dagtid	2	1	2	1	1	1	0	2	0	0
Alltid ansluten	1	0	2	0	0	0	0	1	1	0

Alternativ	Kön (antal)		
	Män	Kvinnor	Totalt
Aktivt använder	5	8	13
Under dagtid	5	5	10
Alltid ansluten	4	1	5

Fråga 10

År	Års erfarenhet med datorer (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
0-1	0	0	0	0	0	0	0	1	0	0
1-3	1	0	0	0	0	0	0	2	1	1
3-6	0	0	1	1	1	2	0	1	0	0
6-	2	1	4	3	2	0	0	2	2	0

År	Kön (antal)		
	Män	Kvinnor	Totalt
0-1	0	1	1
1-3	2	3	5
3-6	2	4	6
6-	10	6	16

Fråga 11

Aktivitet/tjänst	Användning av aktiviteter och tjänster (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Maila	3	1	4	4	3	2	0	5	3	0
Chatta	3	0	4	2	2	1	0	1	0	0
Beställa	2	0	4	4	3	2	0	3	2	0
Banktjänster	2	0	4	3	2	2	0	5	2	1
Söka info	3	1	5	4	3	2	0	5	2	0
Ladda ner	3	0	5	2	2	1	0	1	1	0
Fildelning	3	0	5	1	2	0	0	0	1	0
Spela spel	2	0	4	0	1	1	0	2	0	0
Planlöst surf.	3	0	4	1	1	1	0	1	0	0
Annat	1	0	2	0	0	0	0	0	1	0

Aktivitet/Tjänst	Kön (antal)		
	Män	Kvinnor	Totalt
Maila	13	12	25
Chatta	9	4	13
Beställa	11	9	20
Banktjänster	10	11	21
Söka info	13	12	25
Ladda ner	11	4	15
Fildelning	11	1	12
Spela spel	7	3	10
Planlöst surf.	8	3	11
Annat	4	0	4

Fråga 12

Alternativ	Läser regelbundet någon typ av teknisk datortidning (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Ja	0	0	1	0	1	0	0	0	0	0
Nej	3	1	4	4	2	2	0	6	3	1

Alternativ	Kön (antal)		
	Män	Kvinnor	Totalt
Ja	2	0	2
Nej	12	14	26

Fråga 13

Säkerhetsåtgärd	Säkerhetsåtgärder för att skydda sin dator (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Brandvägg	2	1	2	2	1	1	0	5	2	0
Antivirusprogram	3	0	3	3	3	1	0	5	2	1
Osäkra sidor	0	0	0	0	0	0	0	0	0	0
Kryptering	0	0	0	0	1	0	0	0	0	0
Uppdateringar	2	1	4	1	1	1	0	1	2	1
Användarpolicy	1	1	1	0	0	0	0	0	1	0
Annat	0	0	2	0	0	0	0	0	0	0
Inget skydd	0	0	0	0	0	1	0	0	0	0
Vet ej	0	0	1	1	0	0	0	1	1	0

Säkerhetsåtgärd	Kön (antal)		
	Män	Kvinnor	Totalt
Brandvägg	7	9	16
Antivirusprogram	11	10	21
Osäkra sidor	0	0	0
Kryptering	1	0	1
Uppdateringar	9	5	14
Användarpolicy	3	1	4
Annat	2	0	2
Inget skydd	0	1	1
Vet ej	2	2	4

Fråga 14

Hot/Risk	Förklara innebörden av säkerhetsrisken (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Spyware	2	0	4	0	1	1	0	0	2	0
Maskar	2	0	4	1	2	1	0	1	1	0
Portskanning	1	0	4	0	1	0	0	0	2	0
Bakdörr	0	0	4	2	2	0	0	0	2	0
Netbus	1	0	3	0	2	0	0	0	1	0
Trojaner	3	0	5	1	2	0	0	1	2	0

Hot/Risk	Kön (antal)		
	Män	Kvinnor	Totalt
Spyware	9	1	10
Maskar	9	3	12
Portskanning	8	0	8
Bakdörr	8	2	10
Netbus	7	0	7
Trojaner	12	2	14

Fråga 15

Alternativ	Efter att ha laddat hem ett program eller musikfil (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Kör genast	3	0	1	2	0	0	0	0	0	0
Antivirus + kör	0	0	3	1	2	0	0	1	2	0
Skannar + kör	0	0	0	1	0	1	0	1	0	0
Laddar inte hem	0	1	0	0	0	1	0	3	1	1
Annat	0	0	1	0	1	0	0	1	0	0

Alternativ	Kön (antal)		
	Män	Kvinnor	Totalt
Kör genast	4	2	6
Antivirus + kör	7	2	9
Skannar + kö	0	3	3
Laddar inte hem	1	6	7
Annat	2	1	3

Fråga 16

Alt.	Utsatt för virusangrepp (antal)									
	16-24		25-34		35-44		45-54		55-74	
	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Ja	3	0	4	2	3	1	0	3	1	0
Nej	0	0	1	1	0	1	0	0	1	1
Vet ej	0	1	0	1	0	0	0	3	1	0

Alt.	Kön (antal)		
	Män	Kvinnor	Totalt
Ja	11	6	17
Nej	2	3	5
Vet ej	1	5	6

Fråga 17

	Utsatt för intrångsförsök (antal)									
	16-24		25-34		35-44		45-54		55-74	
Alt.	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
Ja	1	0	3	0	1	1	0	0	1	0
Nej	1	0	0	0	0	0	0	2	0	1
Vet ej	1	1	2	4	2	1	0	4	2	0

Alt.	Kön (antal)		
	Män	Kvinnor	Totalt
Ja	6	1	7
Nej	1	3	4
Vet ej	7	10	17

Fråga 18

	Hur säker du anser din dator är (antal)									
	16-24		25-34		35-44		45-54		55-74	
Alt.	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor	Män	Kvinnor
1	0	0	0	1	0	0	0	1	0	0
2	3	0	1	0	0	1	0	0	1	0
3	0	0	1	1	2	0	0	3	0	0
4	0	1	3	0	1	0	0	1	2	0
5	0	0	0	2	0	0	0	2	0	0

(En har inte svarat i åldern 55-74)

Alt.	Kön (antal)		
	Män	Kvinnor	Totalt
1	0	2	2
2	5	1	6
3	3	4	7
4	6	2	8
5	0	4	4