LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Säkerhetsmedvetande gällande mobila enheter

En kvantitativ studie utförd på privatpersoner

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Felix Conradson
Stefan Markides

Handledare: Umberto Fiaccadori

Examinatorer: Björn Johansson
Bo Andersson

Säkerhetsmedvetande gällande mobila enheter: En kvantitativ studie utförd på privatpersoner

Författare: Felix Conradson och Stefan Markides

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 39

Nyckelord: Mobila enheter, informationssäkerhet, säkerhetsmedvetande, åtgärder

Sammanfattning (Max. 200 ord):
Information är en värdefull tillgång, och att garantera dess säkerhet är en konstant utmaning för alla inblandade. Nuförtiden säljs det fler avancerade mobila enheter än datorer per år, men säkerheten i dessa enheter släpar efter jämfört med säkerheten som erbjuds för datoranvändare. Syftet med denna uppsats är att ta reda på hur medvetna användare är kring säkerhetsrisker som berör mobila enheter, samt i vilken utsträckning de vidtar säkerhetsåtgärder mot dessa risker. Detta har åstadkommits genom att utföra en enkätundersökning, vilken sedan analyserats och därigenom givit oss en överblick över den rådande situationen. Resultaten pekar mot att säkerhetsmedvetandet kring mobila enheter är väldigt lågt, och att i många fall ignoreras riskerna. Enkätsvaren understryker behovet att öka medvetenheten kring säkerheten i deltagarnas personliga enheter. I uppsatsen tas det även upp olika hot och säkerhetsåtgärder, i ett försök att bidra till ökad medvetenhet.

Innehåll

1 Introduktion 4
1.1 Inledning 4
1.2 Problemområde 5
1.3 Syfte och frågeställning 6
1.4 Målgrupp 6
1.5 Avgränsningar 6
2 Teoretiskt ramverk 7
2.1 Vad är en smartphone respektive surfplatta? 7
2.2 Mobilt malware 7
2.3 Bluetooth och dess risker 8
2.4 Phishing 9
2.5 Publika WiFi-nätverk ur ett säkerhetsperspektiv 9
2.6 Vikten av att låsa sina mobila enheter 10
2.7 Risker med att låsa upp en mobil enhets operativsystem 10
2.8 Hur kan man som privatperson skydda sig? 11
3 Metod 13
3.1 Motivering av vald metod 13
3.2 Urval 13
3.3 Utformning av enkät 14
3.4 Etiska aspekter 14
4 Empiriskt resultat 15
4.1 Demografi 15
4.2 Allmänna användningsfrågor 16
4.3 Allmänna säkerhetsfrågor 17
4.4 Frågor om antivirus-appar 19
4.5 Frågor om publika WiFi-nätverk 20
4.6 Kännedom om olika attacktyper 22
5 Analys och diskussion 23
5.1 Liten vikt läggs vid skaparen av appar 23
5.2 Många väljer att ignorera riskerna med malware 24
5.3 Låg medvetenhet om risken med Bluetooth 25
5.4 Hög okunskap om risker med upplåsning av operativsystem 25
5.5 Låg medvetenhet gällande olika typer av attacker 25
5.6 Vanligt att ansluta sig till publika WiFi-nätverk 26
6 Slutsats 27

6.1 Framtida forskningsmöjligheter 28
Bilagor 29
Bilaga 1 - Enkätundersökning 29
Referenser 38

1 Introduktion

1.1 Inledning

Informationssäkerhet har varit en utmaning inom informationssystem sedan länge, och forsätter vara det på grund av den hastiga och konstanta utvecklingen av hoten och ökande mängden användare som behöver ta del av den informationen som ska skyddas. Den teknologiska aspekten åsido; den största förändringen inom informationssäkerhet under åren har varit, enligt Dutta och Roy (2008), vårt synsätt och perspektiv. Fokuset var inriktat på teknologi och ansågs vara lösningen till informationssäkerhetens problem. Sen dess har man insett att det även rör sig om en social aspekt som påverkar den övergripande säkerheten, då användare och deras handlingar för att komma åt informationen kan kompromettera dess sekretess, integritet och tillgänglighet.

Under det senaste decenniet har mobila enheter utvecklats till den punkt att i många fall dessa enheter kan ersätta datorer i vardagliga online-rutiner. Allt fler har tillgång till sin mail i mobilen, använder sig av GPS för navigation, betalar räkningar med tjänster som till exempel Swish (enligt deras officiella hemsida så finns det i dagsläget ungefär 4.5 miljoner användare) och mobil bank, och besöker olika sociala medier som Facebook och Twitter. Detta på grund av att prestandan av mobila enheter har ökat avsevärt de senaste åren och priset både för enheter och abonnemang har sjunkit under samma tidsperiod.

Med mobila enheters stigande popularitet stiger även antalet malware som utvecklas med inriktning på dessa enheter. I många fall kan information (exempelvis inloggningsuppgifter) som är svårt för en hackare att komma åt genom en användares dator vara betydligt mer sårbart genom dennes mobila enhet, då säkerhetsnivån ofta är lägre och användaren inte är lika medveten om existerande risker. Enligt en rapport av Symantec från 2012 så ökade årliga globala försäljningen av smartphones från 461.5 miljoner under 2011 till 645 miljoner under 2012, jämfört med 364 miljoner sålda persondatorer sålda under 2011. Mer specifikt, utifrån den årliga SOM-undersökningen i Sverige så beräknas ungefär 95% av befolkningen ha haft

tillgång till mobiltelefon mellan 2010 och 2012. Av dessa ägare av mobiltelefoner, så beräknades 58% under 2012 att ha ägt en smartphone, vilket är en stor ökning sedan 2010, då antalet låg på 20% (Bolin, 2013). Denna utveckling har gjort det avsevärt mer lönsamt för hackare att fokusera på attacker mot mobila enheter, vilket även rapporteras att ha ökat antalet sårbarheter under 2010 med 93.3%. (Symantec, 2012) I dagsläget finns det två miljarder smartphones som används över hela världen (Curran m.fl., 2015).

I denna uppsats har vi valt att undersöka hur privatpersoner ser på informationssäkerhetsfrågor som berör deras personliga mobila enheter där det inte finns en väldefinierad säkerhetspolicy att följa som kan komma att finnas på exempelvis arbetsplatser. Detta gör att vi vill ta reda på hur välinformerade användare är kring de risker som finns och till vilken grad de skyddar sig mot dessa. Med mobila enheter avser vi smartphones och surfplattor.

1.2 Problemområde

Försäljningen av smarta mobiltelefoner har gått om försäljningen av datorer, och allt eftersom användandet av smarta mobiltelefoner och surfplattor har ökat, har även attackerna mot dessa enheter ökat. Den allmänna prisnivån för teknologi har också sjunkit de senaste åren, vilket också bidrar till att allt fler människor har råd att investera i surfplattor och smartphones (Feng, 2013).

Det råder enligt Ngoqo och Flowerday (2015) stor brist på kunskap hos användare angående informationssäkerhet när det kommer till mobila enheter. Då utvecklingen av mobila enheter har skett så fort, och ständigt är i förnyelse där nya tekniker ständigt utvecklas och introduceras, har informationssäkerheten relaterat till mobila enheter kommit något i skymundan, jämfört med den säkerhetsattityd som är råder kring personliga datorer. Den mänskliga faktorn är ofta ansedd som den svagaste länken när det gäller informationssäkerhet och skydda sig mot attacker på system och nätverk (Imgraben m.fl., 2014).

Många av de studier relaterade till mobil säkerhet utgår oftast från ett organisationsperspektiv, exempelvis om företag har policies gällande användningen av mobila enheter hos de

anställda, samt hur väl dessa efterföljs. Därför gör detta att vi finner det viktigt att undersöka privatpersoners säkerhetsmedvetande och de eventuella åtgärder de vidtar för att säkerställa användningen av sina mobila enheter.

1.3 Syfte och frågeställning

Syftet med studien är att identifiera till vilken utsträckning privatpersoner är medvetna om de informationssäkerhetsrisker som föreligger användningen av mobila enheter, samt om de vidtar åtgärder för att skydda sig mot dessa risker. Uppsatsens två frågeställningar som ämnas besvara i uppsatsen är därmed:

- I vilken utsträckning är privatpersoner medvetna om de hot och risker som föreligger användandet av mobila enheter?
- I vilken omfattning väljer privatpersoner att i så fall skydda sig mot dessa hot och risker?

1.4 Målgrupp

Uppsatsen riktar sig främst till de som är intresserade av informationsteknologi, i synnerhet mobila enheter och säkerhetsaspekten kring dessa. Då studien är användarfokuserad kan det även finnas intresse för yrkesverksamma inom IT-säkerhet, för att få en förståelse för hur användarna av mobila enheter förhåller sig till säkerheten kring dessa.

1.5 Avgränsningar

Denna undersökning riktar sig mot huruvida privatpersoner är medvetna om de risker som kan uppstå vid användandet av mobila enheter, och i så fall hur och till vilken mån de skyddar sig mot dessa risker, samt hur de ser på informationssäkerhet kring sina mobila enheter. Således fokuserar vi inte på huruvida de olika mobila tekniker och gränssnitt som används idag kan göras säkrare, utan på användarnas säkerhetsattityder kring sina mobila enheter.

2 Teoretiskt ramverk

2.1 Vad är en smartphone respektive surfplatta?

En smartphone är i grund och botten en mobiltelefon med avancerade funktionaliteter som i många fall kan konkurrera med personliga datorer (PC). Den första smartphone för kommersiellt bruk anses ha varit Simon Personal Communicator som släpptes under 1994 av BellSouth (Ira Sager, 2012), även om termen smartphone inte användes först förrän ett år senare av AT&T.

Den teknologiska utvecklingen som skett under det senaste årtiondet har tillåtit mobila enheter att bli mer bärbara och användbara. I nuläget kan en smartphone ge användaren tillgång till en mängd olika funktioner och finesser som användaren innan behövde ett flertal olika enheter för att komma åt.

Surfplattor kan liknas vid bärbara datorer med pekskärm istället för tangentbord, och på många sätt är väldigt lika smartphones. Operativsystemen är av samma typ som till smartphones, beroende på tillverkare av surfplattan, iPad och iPhone använder iOS som operativsystem, Android-smartphones och Android-surfplattor använder Android som operativsystem, och det samma gäller för Windows Phone och Windows Tablets, som använder Windows 10.

2.2 Mobilt malware

Det första dokumenterade mobilviruset upptäcktes år 2004 av Kaspesky Lab, och gavs namnet Cabir. Sen dess har antalet malware växt proportionellt med mobila enheters ökande popularitet under senaste decenniet. Ordet malware är en förkortning av “Malicious Software”, vilket beskriver mjukvara med illvillig ändamål, och kan användas som en generell term för bland annat “viruses, botnets, worms, and Trojan horses” (Chandramohan &

Kuan Tan, 2012). Majoriteten av malware riktar sig mot Android-platformen, vilket är tydligt i en rapport som publicerats av McAfee under 2012 som visar att av 8000 kända mobila hot så var 7000 specifika för Android (McAfee, 2013).

Utöver malware, utgör spyware en väldigt stor risk för mobila användare, på grund av mängden känslig information som lagras nuförtiden i dessa enheter. Denna programvara arbetar oftast tyst i bakgrunden för att inte bli upptäckt, och under längre tid stjäl information om användaren och dess data (Chandramohan & Kuan Tan 2012).

2.3 Bluetooth och dess risker

Bluetooth kan beskrivas som en trådlös teknologi ämnad för kommunikation på korta avstånd, och används för filöverföringar mellan mobila enheter. Trots att det är en teknik som är avsedd för kommunikation via korta avstånd är det en teknik som är mottaglig för säkerhetsrisker. Riskerna innefattar data-sekretess samt autentisering (Curran m.fl., 2015).

Enligt Kaur (2013) har det blivit allt vanligare att enheter som stödjer Bluetooth utsätts för elakartade angrepp, på grund av de brister som finns i säkerhetsproceduren när två Bluetooth-enheter kopplas samman. Därför har Bluetooth-enheter en stor benägenhet av att bli utsatta för till exempel batteri-utmattning och DoS-attacker. Curran m.fl. (2015) utökar denna lista av olika attacker med bland annat bakdörr-attacker och spridning av virus. Bakdörr-attacker innebär att förövaren attackerar Bluetooth-förbindelsen mellan två mobila enheter, och kan ta kontroll över enheten och övervaka den på avstånd. Detta gör att förövaren får möjlighet till att se och ladda ned all data på enheten, samt komma åt delar på den utsatta enheten som till exempel kameran och nätverksanslutningen. Denna typ av attack är den som kan utgöra störst skada på enheten eftersom enheten är helt exponerad.

Virus, särskilt maskar, kan spridas via Bluetooth genom att masken kan skanna av enheter och upptäcka om Bluetooth-funktionen är påslagen. Är det påslaget skickar masken sig själv till enheten, och en notifikation dyker upp på enhetens skärm och begär om tillstånd för att installera ett program. Ofta accepterar det tilltänkta offret detta utan att riktigt läsa vad som står i notifikationen, och programmet installeras på enheten. Efter att masken infekterat den

utsatta enheten kan den ständigt söka efter andra enheter som har Bluetooth påslaget och därigenom utmatta enhetens batteri mycket snabbt (Curran m.fl., 2015).

2.4 Phishing

Phishing anses som 2000-talets identitetsstöld, och målet med phishing är att komma över känslig data, till exempel brottoffrens personnummer, kreditkortsnummer och inloggningsuppgifter. Attacken utförs oftast genom att förövaren utformar ett mail som ser ut som att det kommer från en legitim källa som till exempel banker och olika myndigheter. I mailet återfinns en länk, som tar offret till en sida som efterliknar originalsidan, men som i själva verket är en fälla, där offret sedan ombeds att fylla i sin information, som till exempel inloggningsuppgifter eller kreditkortsnummer, beroende vilket företags hemsida den felaktiga sidan ska efterlikna. Istället för ett mail kan även falska SMS användas för att lura offret till en felaktig sida (Dunham, 2009).

2.5 Publika WiFi-nätverk ur ett säkerhetsperspektiv

Offentliga WiFi-nätverk och hotspots har på senare år blivit ett väldigt vanligt fenomen på olika allmänna platser, och erbjuds i nuläget av majoriteten av restauranger, barer och flygplatser. Offentliga WiFi-nätverk är en grodrund för attacker mot mobila enheter, då de allt som oftast är okrypterade, vilket innebär att informationen är tillgänglig och kan samlas in av hackare. Det är enkelt att upprätta en hotspot, och ännu lättare att som hackare replikera. Ett café eller köpcentrum kan till exempel erbjuda sina kunder gratis WiFi, utan att kräva ett lösenord för att kunna ansluta sig till nätverket. Detta kan enkelt utnyttjas av förövare genom att klona nätverket och använda samma namn på nätverket som det ursprungliga. Genom denna metod vet kunden inte att den är ansluten till ett falskt nätverk, och förövaren har full kontroll över nätverket och därmed tillgång till den information som finns på det (Watts, 2016). Utöver kloning av nätverk, så kan förövare använda sig av en bärbar dator med programverktyg installerade som snappar upp och omdirigerar nättrafiken genom förövarens dator, och på så sätt kommer åt information innan den når sin destination (Imgraben m.fl., 2014).

2.6 Vikten av att låsa sina mobila enheter

Bärbarheten som moderna mobila enheter erbjuder ses som ett stort framsteg i utvecklingen, men kan även leda till hot i sin enklaste form, nämligen stöld. I dagsläget så lämnar majoriteten av användare aldrig ifrån sig sina mobila enheter under längre perioder, vilket kan leda till att enheten blir stulen på något sätt. I detta fall, om användaren ej har säkrat sin mobila enhet med någon form av låsmekanism, som till exempel låskod, lösenord, mönster eller fingeravtrycksläsare som finns i nyare modeller av smartphones och läsplattor, då riskerar användaren att kompromettera alla konton och data som finns tillgängligt i enheten. Men det är viktigt att notera att säkerhetsnivån av låsfunktionerna på mobila enheter inte garanterat kommer att stoppa en sofistikerad hackare som har gott om tid (Souppaya & Scarfone 2013). Därför har vissa mobila enheter valfria inställningar som raderar all data från enheten vid ett antal felaktiga inloggningsförsök, men även detta är ej felfritt då en mängd raderad data kan återskappas med rätt verktyg.

2.7 Risker med att låsa upp en mobil enhets operativsystem

Att låsa upp enhetens operativsystem, även kallat *Jailbreak* för iOS, respektive *rooting* för Android, innebär att man förbigår de begränsningar som tillverkaren har applicerat i operativsystemet. De vanligaste anledningar till att vissa användare gör denna upplåsningen är:
(Ruggerio & Foote, 2011)

- Få tillgång till betalda appar utan extra kostnad.
- Få tillgång till appar som annars inte finns tillgängliga för deras enhet.
- Skräddarsy mobila gränssnittet som annars har begränsade förändringsmöjligheter.
- Öka funktionaliteten utöver det som erbjuds i medföljande operativsystem.

Att utföra denna handling är inte en direkt säkerhetsrisk i sig, men istället så medkommer en stor risk att installera applikationer av okända utgivare från inofficiella app stores som användaren får tillgång till, samt så riskerar användaren att inte kunna ta del av nya uppdateringar som släpps för enheten, då utvecklingen av dessa upplåsningar ofta ligger efter med sina egna uppdateringar. Detta beror på att utvecklarna av mobila enheter konstant gör

det svårare för sina nya versioner att upplåsas. I många fall så blundar användare som låser upp sina operativsystem för medförda risker då de anser att ovanstående anledningar överväger dessa.

Generellt så anses iOS vara en säkrare miljö, då Apple är betydligt mer begränsande i sitt operativsystem, och detta stöds av det faktum att endast en bråkdel av den totala mängden malware för mobila enheter riktar sig mot iOS, och i majoriteten av dessa fallen så riktas dessa malware mot enheter med jailbreak (Imgraben m.fl., 2014).

2.8 Hur kan man som privatperson skydda sig?

Det finns många säkerhetsåtgärder användare kan vidta för att skydda sig mot hot riktade mot mobila enheter, och nedan beskrivs några av dessa.

Vara uppmärksam mot misstänkta mail och sms

Malware kan spridas genom att förövaren skickar mail eller SMS som innehåller farliga länkar. Detta gäller även phishing som skrivits om tidigare, därför är det viktigt att ta en extra titt på mail och SMS av okänd avsändare eller av avsändare som ska föreställa ett företag som innehåller länkar (Ruggiero & Foote, 2011).

Vara noga med vilka appar som installeras

Att som användare läsa på om appen och dess skapare innan den installeras kan vara ett bra sätt att filtrera ut elakartade appar. Att kontrollera vilka delar av enheten appen vill ha åtkomst till är också viktigt. Appar som kräver tillgång till delar av enheten som inte har med appens funktion att göra bör undvikas, då de kan innehålla trojaner och annan malware. Därför anses det vara "best practice" att installera antimalware appar, då dessa tillåter att mjukvaran kontrolleras innan den installeras på enheten (Ruggiero & Foote, 2011).

Stänga av förbindelser när de inte används

Att ha WiFi och Bluetooth avstängt när det inte används är ett bra sätt att skydda sig mot attacker, eftersom förövare kan utnyttja sårbarheter i mjukvara som använder sig av dessa förbindelser (Ruggiero & Foote, 2011).

Aktivera icke-upptäckbart läge för Bluetooth

När Bluetooth är påslaget, är det viktigt att aktivera icke-upptäckbart läge, vilket gör att den mobila enheten inte kan upptäckas av andra Bluetooth-enheter. Därmed kan en förövare eller infekterad enhet hitta enheten (Ruggiero & Foote, 2011).

Undvika att ansluta till publika och okända WiFi-nätverk och hotspots

Förövare kan upprätta falska WiFi-nätverk och genom dessa attackera mobila enheter, och kan söka efter oskyddade enheter på publika WiFi-nätverk (Ruggiero & Foote, 2011). I de fall som anses absolut nodvändiga, så bör användaren ej skicka känslig data över dessa nätverk.

Kortfattat menar Ruggiero & Foote att 3 huvudsakliga strategier bör tillämpas för att motverka digitala brott: Öka ansträngningen som krävs för att begå brottet, öka risken att bli ertappad, samt minimera potentiella belöningsfaktoren för gärningsmannen.

3 Metod

3.1 Motivering av vald metod

Vi har valt att använda oss av en kvantitativ metod, med en enkätundersökning som valt verktyg att genomföra detta. Anledningen till att vi valt en kvantitativ metod är att det ger ett generaliserbart resultat av de svar vi får in, och får en representativ bild av en population (Jacobsen m.fl., 2002), vilket är det vi eftersträvar med studien. Kvantitativa undersökningar lämpar sig även enligt Jacobsen m.fl., (2002) väl när målet är att undersöka omfattning eller frekvens. En nackdel med den valda metoden är att vi inte kan säkerställa att respondenterna förstått eller tolkat frågorna så som vi avsett.

Att få in samma mängd data genom en kvalitativ metod med hjälp av intervjuer hade på grund av tidsbrist varit i princip omöjligt att genomföra. Visserligen kan man genom intervjuer få in mer djupgående svar och data, men detta var inte vad vi var ute efter.

3.2 Urval

Då vår frågeställning berör säkerhetsmedvetande gällande mobila enheter klargjordes det vid utskick av enkäten att respondenterna antingen skall äga en smartphone eller en surfplatta för att kunna ta del i undersökningen. Detta var således det enda kravet för att kunna delta i undersökningen.

Eftersom vi strävade efter att nå ut till så många som möjligt, och eftersom enkäten besvarades elektroniskt, skickades enkäten ut via det sociala nätverket Facebook. Att nå ut till potentiella respondenter via Facebook motiverades även av att vår frågeställning behandlar just privatpersoners säkerhetsmedvetande, och därmed ska inga särskilda förkunskaper vara ett krav för att kunna svara på enkäten. Med detta menar vi att resultaten förmodligen hade sett annorlunda ut om vi till exempel lagt ut enkäten på diverse teknikforum på Internet.

3.3 Utformning av enkät

Den nätbaserade enkätundersökningen är skapad med hjälp av Google Forms och besvarades av totalt 81 personer. Enkäten har delats in i sex olika sektioner med en inledande sektion där demografin av respondenterna kartläggs, med en efterföljande sektion som innehåller allmänna frågor om deras användarvanor gällande mobila enheter. Den tredje sektionen består av frågor som är av allmän säkerhetskaraktär kopplade till mobila enheter. De resterande sektionernas kategorier är uppdelade efter de olika typer av risker och hot som föreligger användandet av mobila enheter, där frågorna i sig är baserade på den teori vi presenterat.

3.4 Etiska aspekter

Jacobsen m.fl. (2002) skriver om ett antal etiska aspekter gällande förhållandet mellan forskare och de som undersöks. Några av dessa aspekter är något vi tagit hänsyn till vid utformandet av enkäten, samt den information vi delgivit respondenterna angående undersökningens syfte. En av dessa aspekter kallas *informerat samtycke*, vilket innebär att den som undersöks av fri vilja ska delta i undersökningen, och att den undersökte vet om de eventuella riskerna och vinsterna deltagandet i undersökningen kan medföra. Detta realiserade vi genom att vi vid utskick av enkäten beskrev vad dess syfte var, samt att vi skrev att det handlade om säkerhetsmedvetande gällande mobila enheter. Självklart kan man inte exakt skriva hur svaren kommer att användas, då *full information* kan få stora effekter på en undersöknings tillförlitlighet, då respondenten kan komma anpassa sina svar därefter (Jacobsen m.fl., 2002).

Även att de som undersöks ska ha *rätt till ett privatliv* togs hänsyn till. Vi garanterade full anonymitet gentemot våra respondenters identitet, vilket vi informerade om i samband med utskick av enkäten. Då vi använde oss av Google Forms säkerställdes detta, där det är omöjligt att sammankoppla svar på enkäten till en persons identitet.

4 Empiriskt resultat

I detta avsnitt kommer vi att presentera de viktigaste resultaten av den empiri vi samlat in genom enkäten. Analys och diskussion om resultaten sker i avsnittet efter. Vissa svar tas endast upp för att jämföras med andra svar och se om något samband kan etableras, då dessa svar inte är indikativa på egen hand.

4.1 Demografi

Totalt 81 personer deltog i enkäten. En stor majoritet av deltagare (44.4%) var mellan 18 och 25 år gamla och av dessa är 83.3% studerande eller nyligen avklarade med studier. Kvinnor utgjorde 60.5% av totala deltagare.

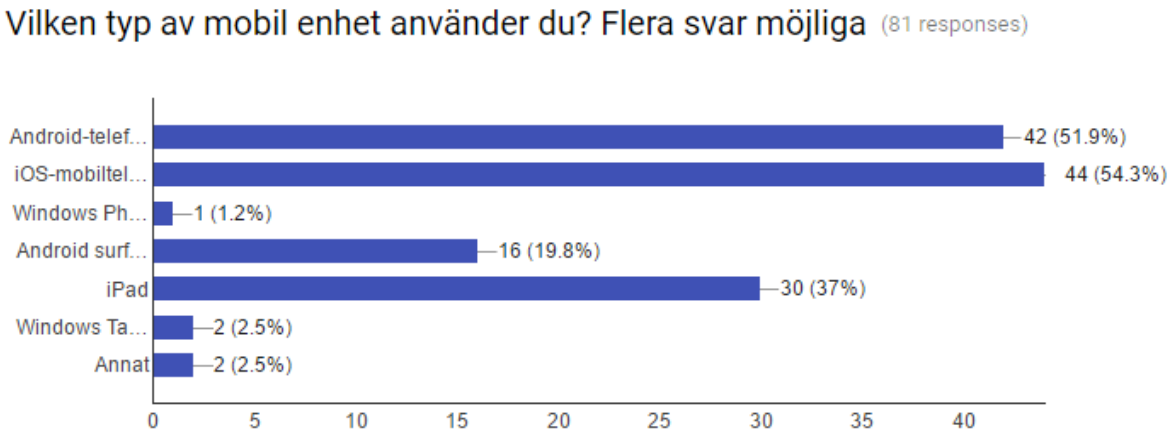
Ålder	Total (81)
Under 18	7 (8.6%)
18-25	36 (44.4%)
26-35	13 (16%)
36-50	13 (16%)
51+	12 (14.8%)

Kön	Total (81)
Man	32 (39.5%)
Kvinna	49 (60.5%)

Utbildningsnivå	Total (81)
Grundskola	5 (6.2%)
Gymnasieutbildning	14 (17.3%)
Eftergymnasial utbildning	62 (76.5%)

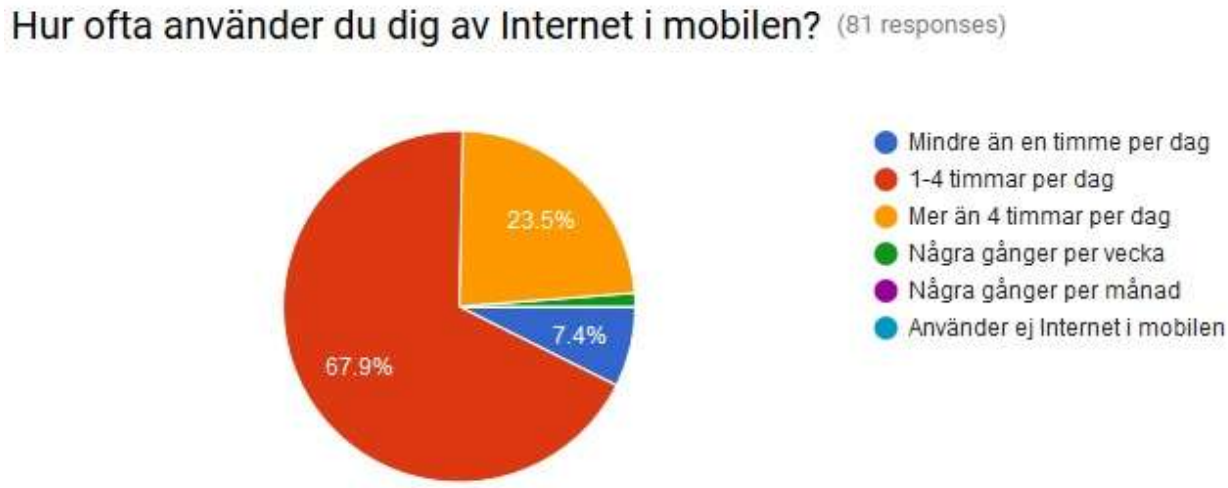
Tabell 4.1 *Demografi*

4.2 Allmänna användningsfrågor



Figur 4.1 *”Vilken typ av mobil enhet använder du? Flera svar möjliga”*

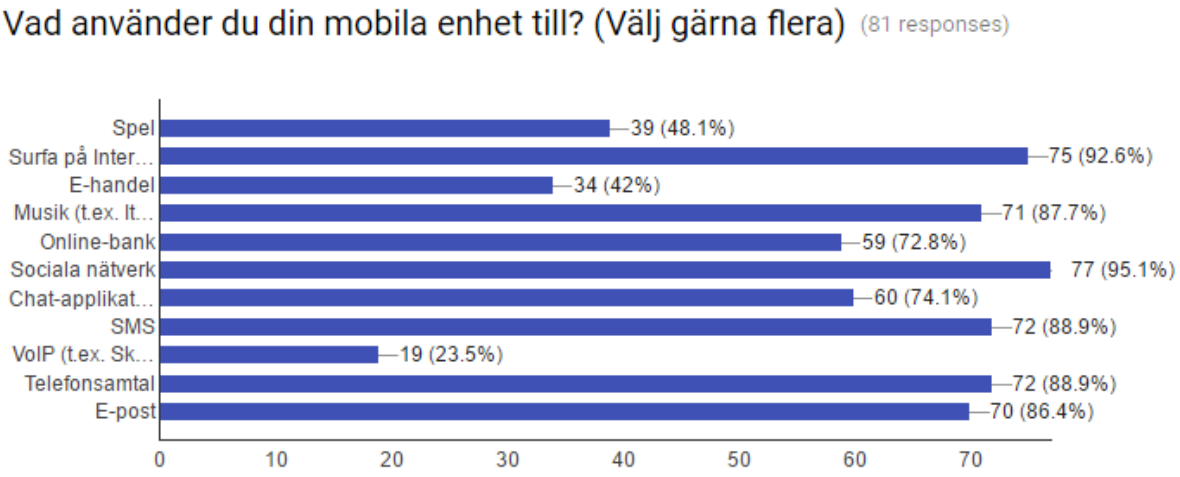
Då denna fråga tillät deltagarna att välja ett flertal av mobila enheter, så överskrider antalet mobila enheter antalet deltagare, men främst i form av kombinationer av en smartphone och en surfplatta. På frågan om vilken typ av smartphone respondenterna använder var det väldigt jämnt mellan iPhone och Android, med en liten fördel för iPhone med 54% respektive 51%, vilket innebär att några av respondenterna använder båda typer av smartphone. Ett fåtal respondenter använder Windows Phone eller annan typ av smartphone. iPad var den vanligaste surfplatta med 37% av deltagare, i motsats till 19.8% som äger Android-surfplatta och 2.5% Windows Tablet.



Figur 4.2 *”Hur ofta använder du dig av Internet i mobilen?”*

Majoriteten av respondenterna använder Internet i sin mobila enhet “en till fyra timmar per dag” (67.9%), följd av “fyra eller fler timmar per dag” (23.5%) och mindre grupper som

uppgörs av sällananvändare. En tydlig relation mellan ålder och användning kan observeras, då de yngre åldersgrupper var betydligt mer sannolika att använda internet i mobila enheter i 4 timmar eller fler per dygn, medans majoriteten av de äldre grupperna (36-50 och 51+) använder internet mellan en och 4 timmar per dag eller mindre (72%).



Figur 4.3 *”Vad använder du din mobila enhet ditt?”*

Vi ville även ta reda på vad deltagarna använder sina mobila enheter till, för att få en idé om vilka hot de kan möjligtvis utsättas för samt vilken data kan kompromitteras. Online-kommunikation är främsta användningen enligt resultatet av frågan om användning, med konton som e-post, sociala nätverk och chat-applikationer som populärast. Vid vår fråga om vilka konton som blivit utsatta vid någon sort av säkerhetsbrist, var det även dessa som var de vanligaste att bli stulna.

4.3 Allmänna säkerhetsfrågor

För att få en överblick över respondenternas säkerhetsattityd ställde vi i tredje sektionen av enkäten frågor som behandlade säkerhetsattityden på ett generellt plan.

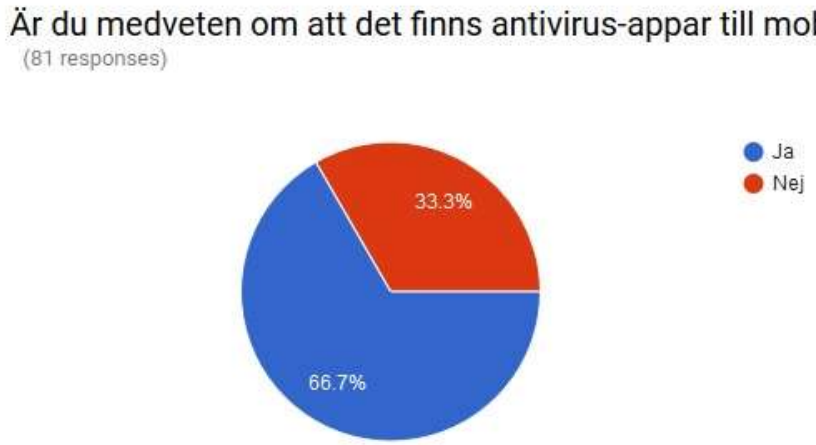
Figur 4.4 ”*Hur eller lågt anser du själv ditt säkerhetsmedvetande gällande mobila enheter vara?”*

Majoriteten av respondenterna anser sig själva ligga på en lagom till hög nivå av säkerhetsmedvetande gällande mobila enheter. Denna fråga ställdes tidigt i enkäten även om den ej är avgörande främst för att kunna jämföra respondenternas egna uppfattning av sin säkerhetsmedvetande och den nivå den egentligen ligger på.

Figur 4.5 *”Använder du lösenkod för att låsa upp din mobila enhet?”*

En stor majoritet av deltagarna använder sig av någon form av lösenkod (84%), men 16% är en hög nog siffra för att skapa oro, specifikt när denna statistik jämförs med antalet av dessa personer som svarade med högre sannolikhet att lämna sin mobila enhet obevakad i offentliga miljöer.

4.4 Frågor om antivirus-appar



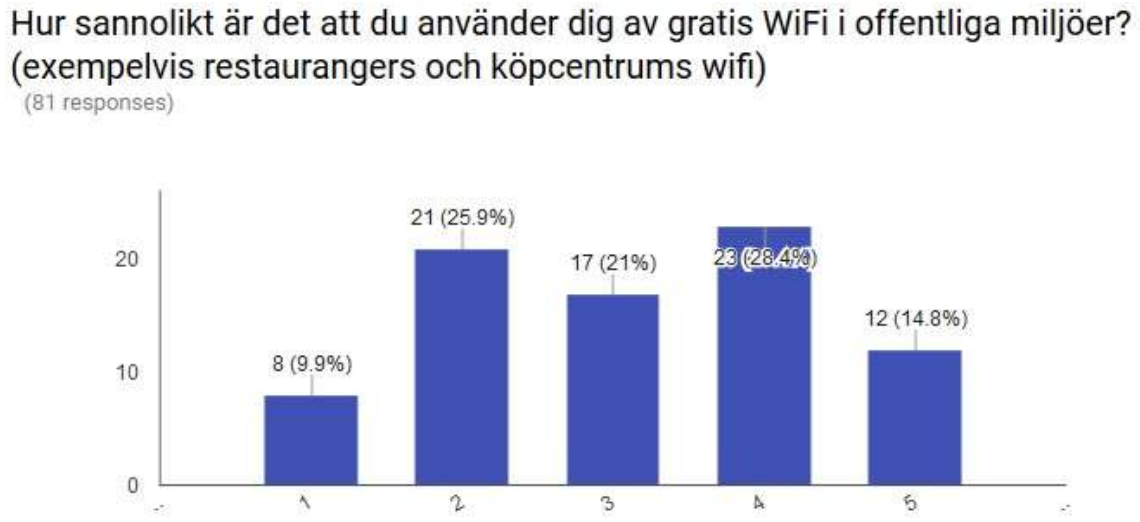
Figur 4.6 ”*Är du medveten om att det finns antivirus-appar till din mobila enhet?”*

Majoriteten av de svarande vet om att det finns antivirus-appar till mobila enheter.

Figur 4.7 *”Använder du dig av någon antivirus-app i någon av dina mobila enheter?”*

En viktig fråga som undersöker respondenternas tendenser att skydda sina mobila enheter mot virus med hjälp av en antivirus-app. Drygt 70% av de tillfrågade använder sig inte av antivirusskydd i sina mobila enheter, och cirka 12% vet inte om de använder sig av detta.

4.5 Frågor om publika WiFi-nätverk

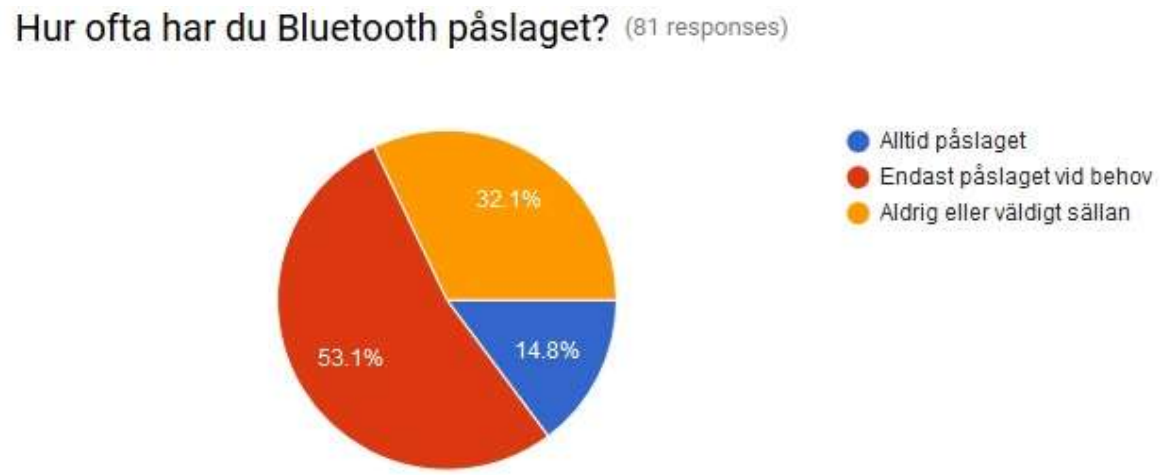


Figur 4.8 *"Hur sannolikt är det att du använder dig av gratis WiFi i offentliga miljöer?"*

För 29 stycken (sannolikhetsnivå 1 och 2) av de tillfrågade är det mindre sannolikt att de ansluter sig till offentliga WiFi-nätverk, medan 35 av de tillfrågade finner det mer sannolikt att de ansluter sig till offentliga WiFi-nätverk (sannolikhetsnivå 4 och 5). Resterande 17 respondenter finner det sannolikt att de ansluter sig till offentliga WiFi-nätverk (sannolikhetsnivå 3). För denna fråga använde vi oss alltså av en likertskala där 1 motsvarar mycket osannolike och 5 motsvarar mycket sannolikt.

Figur 4.9 *"Hur hög eller låg anser du risken vara med att ansluta sig till öppet WiFi?"*

43% av respondenterna anser att risken med att ansluta sig till öppna WiFi-nätverk är hög, medan knappt 30% anser risken vara låg. 17% av de tillfrågade säger sig inte veta om de anser risken vara hög eller låg.



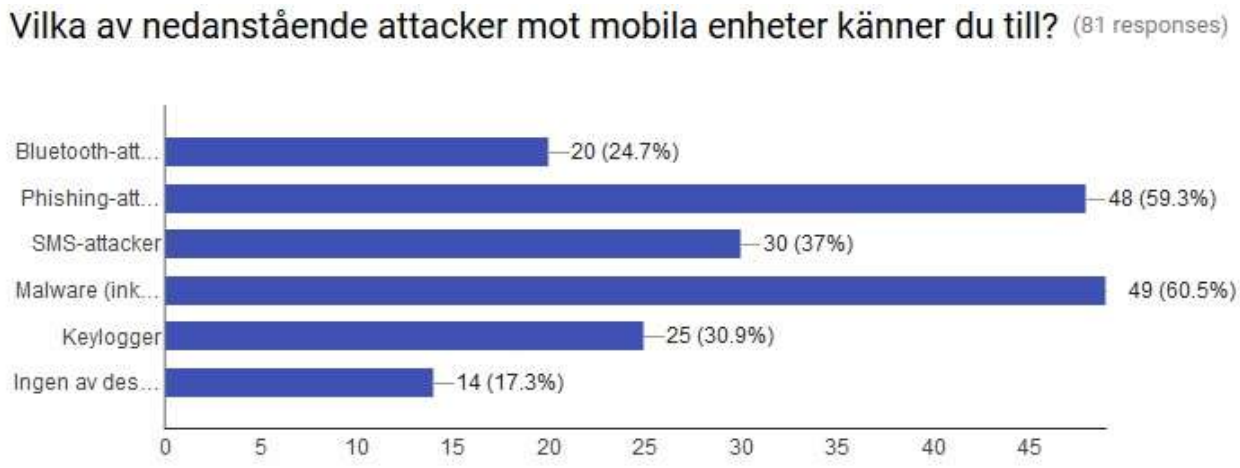
Figur 4.10 ”*Hur ofta har du Bluetooth påslaget?”*

Drygt hälften av de tillfrågade har Bluetooth påslaget endast vid behov, medan 32% aldrig eller väldigt sällan har Bluetooth påslaget. Resterande 14% har alltid Bluetooth påslaget.

Figur 4.11 *”Hur stor vikt lägger du vid skaparen av den app du vill ladda ner?”*

Över hälften av respondenterna säger sig lägga liten vikt vid skaparen av appen de laddar ner, och nästan en fjärdedel säger sig lägga ingen vikt alls vid detta.

4.6 Kännedom om olika attacktyper



Figur 4.12 *”Vilken av nedanstående attacker mot mobila enheter känner du till?”*

Denna fråga undersöker vilka attack-typer de tillfrågade känner till. Resultatet visar att 60% känner till både phishing-attacker och malware, och var således de två mest välkända attacktyperna. Bluetooth-attacker, SMS-attacker och Keyloggers var ungefär lika välkända, som kändes igen av cirka 30% av de tillfrågade. 17% av de tillfrågade kände inte till någon av de listade attack-typerna.

5 Analys och diskussion

På frågan om respondenternas egna uppfattning om deras säkerhetsmedvetande fick de svara på en likertskala mellan 1 och 5, där 1 motsvarar mycket låg och 5 motsvarar mycket hög. Majoriteten ansåg sig själv ligga på nivå 3, det vill säga varken ett högt eller lågt säkerhetsmedvetande.

5.1 Liten vikt läggs vid skaparen av appar

Över 50 procent av de som svarat på enkäten lägger liten vikt vid tillverkaren av appar när de väljer att ladda ner och installera appar, vilket tyder på ett bristande säkerhetsmedvetande, då appar kan innehålla malware. Detta är visserligen vanligare bland mindre kända appar, men att över 50% påstår sig lägga liten vikt vid detta bör ändå anses som allt för lågt ur ett säkerhetsperspektiv. Användare som vid något tillfälle låst upp sitt operativsystem uppvisade generellt sämre säkerhet utifrån svaren de angett i enkäten. Bland annat så var de mer benägna att inte lägga vikt på tillverkaren av appar, majoriteten tillät sidor spara inloggning- och betaldetaljer samt var under genomsnittet vid frågan om de hade antivirusappar.

På frågan om vilka olika typer av attacker mot mobila enheter respondenterna kände till var det endast 60 procent av de tillfrågade som var medvetna om att det finns malware, där även virus ingår, som förmodligen är en mer känd term, vilken vi också nämnde i enkätfrågan. Vid jämförelse med de personer som svarat att de lägger liten eller ingen vikt på tillverkaren av appen så kan ett tydligt samband etableras då 72.4% av dessa svarade att de även inte kände till malware. Detta pekar mot en stor brist inom säkerhetsmedvetande gällande mobila enheter då dessa användare ej är medvetna om att appar som till synes verkar vara legitima istället kan vara laddade med malware av någon sort. Även om användaren inte har låst upp operativsystemet på sin mobila enhet (jailbreak/rooting), är det inte tillräckligt att lita på att till exempel Apple App Store och Android utvärderar och eliminerar illvilliga applikationer,

då det har förekommit fall där tiotusentals nedladdningar av en viss applikation skett förrän det upptäckts att innehålla skadlig kod (Ruggerio & Foote, 2011).

Det är dock viktigt att påpeka att även applikationer utgivna av respektabla utvecklare kan användas i illvilliga syften då många av dessa inte är helt säkrade och det kan förekomma ett antal sårbarheter för hackare att utnyttja som bakväg in i den mobila enheten (Souppaya & Scarfone 2013). Enligt John Cox, så är detta möjligt med något så enkelt som en bakgrundsapplikation med viss sårbarhet på ett okrypterade nätverk, och dessa okrypterade nätverk finns tillgängliga nästan överallt. Allt hackaren behöver göra är att omdirigera nätverkstrafiken genom en bärbar dator, och kan på så sätt få tillgång till all data som användaren skickar och tar emot över nätverket, och på så sätt kan ignorera SSL-certifikat som annars krypterar datan användaren skickar och tar emot (Symantec, 2014).

5.2 Många väljer att ignorera riskerna med malware

Trots att 67% av respondenterna är medvetna om att det finns antivirus-appar för mobila enheter, svarade bara 16% att de faktiskt använder sig av en antivirus-app. Detta kan tolkas som en relativt hög medvetenhet hos respondenterna om att det existerar virusskydd för mobila enheter, men att de flesta trots detta väljer att ignorera det hotet, och väljer att inte skydda sig mot denna typ av attack. Malware anses vara ett av de största hoten mot mobila enheter. Vi lade även märke till att majoriteten av antivirus-användare har tidigare varit utsatta för någon sorts intrång eller förlust av data i sin mobila enhet, vilket pekar mot en reaktiv och inte proaktiv inställning mot informationssäkerhet i mobila enheter. Då en del av syftet med att undersöka till vilken mån privatpersoner skyddar sig mot hot, är alltså malware en typ av hot man oftast inte skyddar sig mot, trots att majoriteten vet om att det finns antivirus-appar tillgängliga för mobila enheter.

Över 70% av respondenterna anser att det är en stor chans att de skulle kunna identifiera ett phishing-försök i form av ett falskt e-mail, vilket får anses som ett relativt högt säkerhetsmedvetande gällande denna typ av hot, men att redogöra för hur detta ter sig i verkligheten är dock svårt att avgöra.

Det kan sägas att diskrepansen mellan säkerhetsmedvetandet och att faktiskt skydda sig mot hot och risker gällande informationssäkerhet är relativt hög, det vill säga även om det finns en hyfsat god medvetenhet kring riskerna med mobila enheter, väljer många att inte skydda sig mot dessa.

5.3 Låg medvetenhet om risken med Bluetooth

I litteraturen är attacker som möjliggörs av Bluetooth-tekniken ett ständigt återkommande område, men kunskapen om Bluetooth-attacker är enligt våra resultat mycket låg, då endast en fjärdedel av de tillfrågade känner till att Bluetooth faktiskt kan utgöra sårbarheter på deras mobila enheter. Visserligen har hälften av de svarande endast Bluetooth påslaget vid behov, men baserat på den låga medvetenheten om Bluetooths sårbarhet, tror vi att detta till stor del beror på andra anledningar än av just säkerhetsskäl, som att man till exempel vill spara på batteriet i sina mobila enheter, eller att man sällan har behov av Bluetooth-tekniken.

5.4 Hög okunskap om risker med upplåsning av operativsystem

Över hälften av de tillfrågade är omedvetna om huruvida säkerheten i en mobil enhet kompromissas vid upplåsning av operativsystemet, och även om majoriteten av de svarande inte har låst upp operativsystemet på sina enheter, och därmed inte själva blir utsatta för en större risk att bli infekterade på detta sätt, vittnar resultaten om att okunskapen är mycket hög om denna typ av risk. Att majoriteten inte har låst upp operativsystemet tror vi mest är ett resultat av en blandning av okunskap om hur operativsystemet upplåses, samt ren ovilja att komma åt de funktioner upplåsningen medför, och behöver inte nödvändigtvis vara en fråga om säkerhet för de svarande.

5.5 Låg medvetenhet gällande olika typer av attacker

Det råder en stor skillnad mellan vilka attack-typer respondenterna känner till, då 60% av deltagarna känner till phishing och malware, medan endast 24% respektive 37% känner till Bluetooth-attacker och SMS-attacker. 14 personer av de 81 tillfrågade känner inte till någon

av de fem attack-typer vi listat. Dessa siffror visar på ett överlag lågt säkerhetsmedvetande och kunskap hos respondenterna gällande attacker mot mobila enheter.

Enligt Ngoqo & Flowerday (2015) finns det inte mycket som tyder på att användare av mobila enheter har någon kunskap om informationssäkerhet, eller att de tillämpar något säkerhetstänk. Detta stämmer överens till viss grad med våra resultat, även om det inte är riktigt lika illa som Ngoqo och Flowerday åberopar det vara, då vi ändå fann ett visst säkerhetsmedvetande hos respondenterna, även om det lämnar mycket att önska.

5.6 Vanligt att ansluta sig till publika WiFi-nätverk

En stor del av respondenterna anser det vara sannolikt att de kopplar upp sig mot offentliga WiFi, samtidigt som 43% anser att risken med offentliga WiFi-nätverk är hög. Detta visar på ett visst mått av säkerhetsmedvetande gällande öppna WiFi-nätverk, men benägenheten att avstå från att koppla upp sig mot sådana nätverk är låg.

Denna fråga kunde i efterhand formulerats bättre; istället för att uppskatta sannolikheten i att koppla upp sig mot öppna WiFi-nätverk skulle vi kunnat fråga hur ofta de gör detta. Då hade vi fått ett tydligare svar som varit enklare att dra slutsatser från, men slutresultatet av frågan hade troligtvis varit väldigt snarlik; det vill säga att de flesta brukar koppla upp sig mot publika WiFi-nätverk.

6 Slutsats

Uppsatsens syfte var att identifiera till vilken utsträckning privatpersoner är medvetna om de informationssäkerhetsrisker som föreligger användningen av mobila enheter, samt till vilken mån de vidtar åtgärder för att skydda sig mot dessa risker. Detta har enligt oss uppfyllts, då vi genom enkäten undersökt dessa frågor och fått en generaliserad bild över respondenternas säkerhetsmedvetande och till vilken mån de väljer att skydda sig. Överlag råder det ett lågt säkerhetsmedvetande gällande de typer av attacker som riktas mot mobila enheter och de risker som tillkommer vid olika typer av användningsförfaranden, som att till exempel koppla upp sig mot öppna WiFi-nätverk. Den omfattningen i vilken de svarande skyddar sig mot hot och risker har också visat sig varit alltför låg, sett till de användningsområden de svarande använder sina mobila enheter till.

Andelen som vet om att det finns antivirus-appar för mobila enheter korrelerar illa med den andel som faktiskt använder sig av sådana appar. Detta är något förvånande, då det tydligt visar på en ignorans gentemot risken med virus till mobila enheter, och därmed ett lågt säkerhetsmedvetande och låg säkerhetsattityd mot mobila virus, samtidigt som virus och malware mot mobila enheter anses vara ett av de största hoten enligt respondenterna själva.

Av de 20 personer som säger sig blivit utsatta för intrång på sina mobila enheter, svarade sju stycken på vilka åtgärder de vidtog för att förbättra sin säkerhet. Dessa var bland annat byte av lösenord och att installera antivirus-appar i enheten.

Ett återkommande mönster som är av stor relevans sett till uppsatsens två frågeställningar vi sett vid analys av empirin är att även om majoriteten är medvetna om riskerna med ett visst hot, väljer de att ändå inte vidta några åtgärder mot dessa. Detta kan ses i fallet där en majoritet anser att risken med att ansluta sig till offentliga WiFi-nätverk, men att de flesta trots detta anser att möjligheten att få tillgång till Internet ändå väger över den eventuella risken med att ansluta sig till ett offentligt WiFi-nätverk. Liknande tendenser går att återfinna

i frågan om antivirusskydd för mobiler, där över hälften är medvetna om att det finns antivirus-appar, men att merparten ändå svarat att de inte använder sig av sådana appar.

Liknande resultat kan enligt Ngoqo och Flowerdale (2015) återfinnas i Androulidakis och Kandus studie från 2011, där användare av mobila enheter i vissa fall var medvetna om hot man kan utsättas för, men att vidta några säkerhetsåtgärder inte var till någon större angelägenhet för dessa användare. Detta förklaras av Androulidakis & Kandus med att användarna är omedvetna om vilka åtgärder som kan vidtas för skydda sig mot intrång.

Vidare visar våra resultat att medvetenheten och diskussionen om hot mot mobila enheter bör höjas, då användandet av mobila enheter, som tidigare nämnts, bara ökar och har redan gått om försäljningen av datorer (Want, 2009). Mobila enheter är idag så pass avancerade att de i mångt och mycket kan ersätta behovet av vanliga datorer för många människor.

6.1 Framtida forskningsmöjligheter

Vår uppsats bidrar med en analys av hur säkerhetsmedvetandet ser ut i dagsläget, men det öppnar många frågor för framtida forskning;

- Vilka åtgärder utöver de vi nämner i denna uppsats kan privatpersoner tillämpa för att öka säkerheten för sina mobila enheter?

- Vad behövs göras för att öka säkerhetsmedvetandet hos privatpersoner då detta är fortfarande väldigt lågt jämfört med motsvarande medvetenhet kring datorsäkerhet?

- Vad kan utvecklare göra för att öka skyddet för omedvetna användare som främst uppgörs av oerfarna och sporadiska användare, dessutom utan att kräva hög teknisk kompetens av användaren?

- Begränsa studier till specifika folkgrupper för att identifiera de mest utsatta användarna.

Bilagor

Bilaga 1 - Enkätundersökning

Enkätundersökning kring säkerhetsmedvetande hos privatpersoner gällande mobila enheter

Denna enkätundersökning behandlar frågor om informationssäkerhet kring mobila enheter, och vänder sig således till dig som äger en smartphone eller surfplatta. I undersökningen används begreppet "mobil enhet", vilket avser smartphone eller surfplatta, alltså inte laptops. Enkäten är helt anonym, och de svar på enkäten som behandlas innehåller ingen information som kan identifiera den som svarat.

Demografi

Vilket kön tillhör du? *

- ○ Man
- ○ Kvinna

Hur gammal är du? *

- ○ Under 18
- ○ 18-25
- ○ 26-35
- ○ 36-50
- ○ 51+

Hur hög eller låg anser du din datorvana vara på en skala på 1-5, där 1 motsvarar mycket låg och 5 motsvarar mycket hög? *

	1	2	3	4	5	
Mycket låg	○	○	○	○	○	Mycket hög

Vilken är din högsta utbildningsnivå? *

- ○ Grundskola
- ○ Gymnasieutbildning
- ○ Eftergymnasial utbildning

Allmänna Frågor

Vilken typ av mobil enhet använder du? Flera svar möjliga *

- [ ] Android-telefon
- [ ] iOS-mobiltelefon
- [ ] Windows Phone
- [ ] Android surfplatta
- [ ] iPad
- [ ] Windows Tablet
- [ ] Annat

Hur ofta använder du dig av Internet i mobilen? *

- ○ Mindre än en timme per dag
- ○ 1-4 timmar per dag
- ○ Mer än 4 timmar per dag
- ○ Några gånger per vecka
- ○ Några gånger per månad
- ○ Använder ej Internet i mobilen

Vad använder du din mobila enhet till? (Välj gärna flera) *

- [ ] Spel
- [ ] Surfa på Internet
- [ ] E-handel
- [ ] Musik (t.ex. Itunes, Spotify, Tidal)
- [ ] Online-bank
- [ ] Sociala nätverk
- [ ] Chat-applikationer
- [ ] SMS
- [ ] VoIP (t.ex. Skype, Viber)
- [ ] Telefonsamtal
- [ ] E-post

Allmänna säkerhetsfrågor

Hur högt eller lågt anser du själv ditt säkerhetsmedvetande gällande mobila enheter vara på en skala på 1-5, där 1 motsvarar mycket lågt och 5 motsvarar mycket högt? *

	1	2	3	4	5	
Mycket lågt	○	○	○	○	○	Mycket högt

Använder du lösenkod för att låsa upp din mobila enhet? (Även fingeravtryck, mönster osv.) Ej att förväxla med PIN-kod till SIM-kort. *

- ○ Ja
- ○ Nej

Hur sannolikt är det att du skulle lämna din mobila enhet obevakad i offentliga miljöer, på en skala 1-5 där 1 är mycket osannolikt och 5 är mycket sannolikt? *

	1	2	3	4	5	
Mycket osannolikt	○	○	○	○	○	Mycket sannolikt

Är du medveten om att det finns antivirus-appar till mobila enheter? *

- ○ Ja
- ○ Nej

Använder du dig av någon antivirus-app i någon av dina mobila enheter? *

- ○ Ja
- ○ Nej
- ○ Vet inte

Vid inloggning på olika online-tjänster, tillåter du att sidan "kommer ihåg" dina inloggningsuppgifter? *

- ○ Ja
- ○ Nej
- ○ Ibland
- ○ Aldrig

Offentliga Nätverk

Hur ofta har du WiFi-funktionen påslaget i din mobila enhet? *

- ○ Alltid
- ○ Endast vid behov
- ○ Aldrig eller väldigt sällan

Hur sannolikt är det att du använder dig av gratis WiFi i offentliga miljöer? (exempelvis restaurangers och köpcentrums wifi) *

	1	2	3	4	5	
Mycket osannolikt	○	○	○	○	○	Mycket sannolikt

Hur sannolikt är det att du använder dig av öppet WiFi för att logga in på sidor med känslig information (till exempel sociala medier, mail-konto, online-bank)? *

	1	2	3	4	5	
Mycket osannolikt	○	○	○	○	○	Mycket sannolikt

Hur hög eller låg anser du risken vara med att ansluta sig till öppet WiFi? *

- ○ Mycket hög
- ○ Hög
- ○ Låg
- ○ Mycket låg
- ○ Vet inte

Anser du att den eventuella risken med öppna WiFi-nätverk överväger möjligheten att få tillgång till internetuppkoppling? *

- ◯ Ja
- ◯ Nej
- ◯ Vet inte

Hur ofta har du Bluetooth påslaget? *

- ◯ Alltid påslaget
- ◯ Endast påslaget vid behov
- ◯ Aldrig eller väldigt sällan

Appar

Har du någonsin låst upp operativsystemet på din mobila enhet med hjälp av till exempel Jailbreak eller rooting? *

- ◯ Ja
- ◯ Nej
- ◯ Vet ej

Tror du att säkerheten för din mobila enhet generellt försämras vid upplåsning av operativsystemet? *

- ◯ Ja
- ◯ Nej
- ◯ Vet inte

Hur stor vikt lägger du vid skaparen av den app du vill ladda ner? (ur ett säkerhetsperspektiv) *

- ◯ Ingen vikt
- ◯ Liten vikt
- ◯ Stor vikt
- ◯ Vet ej

Hur ofta brukar du lägga märke till vilka delar av din mobila enhet en viss app vill ha tillgång till? *

- ○ Alltid
- ○ Ofta
- ○ Ibland
- ○ Sällan
- ○ Aldrig
- ○ Vet ej

Risker

Vilka av nedanstående attacker mot mobila enheter känner du till? *

- ☐ Bluetooth-attacker
- ☐ Phishing-attacker
- ☐ SMS-attacker
- ☐ Malware (inklusive virus)
- ☐ Keylogger
- ☐ Ingen av dessa

Vilket av dessa ovanstående attacker anser du vara den största risken med att använda mobila enheter? (Välj en) *

- ○ Bluetooth-attacker
- ○ Phishing-attacker
- ○ SMS-attacker
- ○ Malware (inklusive virus)
- ○ Keylogger
- ○ Vet inte

Hur stor chans tror du det är att du skulle kunna identifiera ett falskt mail på din mobila enhet som ber om dina inloggningsuppgifter (Phishing)? *

- ○ Stor chans
- ○ Liten chans
- ○ Vet ej
- ○ Läser inte mail på mobil enhet

Har du någonsin råkat ut för phishing? *

- ○ Ja
- ○ Nej
- ○ Vet ej

Om ja, vilka av dessa konton blev utsatta?

- ☐ Sociala medier
- ☐ Epost/Chat applikationer
- ☐ Bankkonto
- ☐ Annat
- ☐ Inga konsekvenser

Har du någonsin blivit utsatt för obehörigt intrång på din mobila enhet? *

- ○ Ja
- ○ Nej
- ○ Vet ej

Om ja, hur många gånger har det inträffat?

- ○ 1 gång
- ○ 2-3 gånger
- ○ Fler än 3 gånger

Om du blivit utsatt för intrång, vilka konsekvenser fick intrånget? (Fler svar möjliga)

- [ ] Övertag av sociala medier
- [ ] Övertag av e-mail
- [ ] Övertag av personliga filer
- [ ] Övertag av bankkonto
- [ ] Other: _____

Om du blivit utsatt för intrång, vidtog du några åtgärder för att förbättra din säkerhet efter intrånget/intrången?

- ○ Ja
- ○ Nej

Om du vidtog några åtgärder, specifiera vad du gjorde för att förbättra din säkerhet.

Your answer

Referenser

Bolin, G. (2013): *Mobila generationer i Lennart Weibull, Henrik Oscarsson & Annika Bergström (red) Vägskäl. Göteborgs universitet: SOM-institutet.*
http://som.gu.se/digitalAssets/1453/1453901_33-g--ran-bolin.pdf (besökt 2016-04-22)

Chandramohan, M., Kuan Tan, H. (2012): *Detection of Mobile Malware in the Wild*, Computer, vol.45, no. 9, pp. 65-71

Cox, J. (2009): *iPhone on Wi-Fi vulnerable to security attack.* Network World US
http://www.macworld.co.uk/news/apple/iphone-wi-fi-vulnerable-security-attack-27777/ (besökt 2016-06-10)

Curran, K., Maynes, V., Harkin, D. (2015): *Mobile Device Security.* Int. J. Information and Computer Security, Vol. 7, No. 1

Dunham, K (2009): *Mobile Malware Attacks and Defense*. Elsevier Inc.
http://www.sciencedirect.com.ludwig.lub.lu.se/science/article/pii/B978159749298000001X (besökt 2016-05-16)

Dutta, A., Roy, R. (2008) : *Dynamics of organizational information Security*. In: System Dynamics Review, volym 24, nr. 3, sid. 349-375.

Feng, J. (2013): *Attack on WiFi-based Location Services and SSL Using Proxy Servers*. University of Waterloo
https://uwspace.uwaterloo.ca/handle/10012/8116#? (besökt 2016-05-12)

Imgraben, J., Engelbrecht, A., Choo, K. (2014): *Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users.* Behaviour & Information Technology, Vol. 33, No. 12

Jacobsen, D. I., Sandin, G., & Hellström, C. (2002): *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*, Lund : Studentlitteratur, 2002 (Lund : Studentlitteratur)

Kaur, S. (2013). How to Secure Our Bluetooth Insecure World!. *IETE Tech Rev*, 30(2), p.95.

McAfee. 2013. *Mobile Security: McAfee Consumer Trends Report (Trends in risky apps, mobile misbehavior, and spyware).*
http://www.mcafee.com/us/resources/reports/rpmobile-security-consumer-trends.pdf (besökt 2016-05-12)

Ngoqo, B. and Flowerday, S. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security*, 53, pp.132-142.

Ruggerio, P., Foote, J. (2011): *Cyber Threats to Mobile Phones.* US-Cert https://www.us-cert.gov/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf (besökt 2016-05-20)

Sager, I (2012) : *Before iPhone and Android came Simon, the first Smartphone.* Bloomberg L.P. http://www.bloomberg.com/news/articles/2012-06-29/before-iphone-and-android-came-simon-the-first-smartphone (besökt 2016-05-05)

Souppaya, M., Scarfone, K. (2013): *Guidelines for Managing the Security of Mobile Devices in the Enterprise* NIST http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf (besökt 2016-05-18)

Symantec (2014): *How SSL Works* https://www.symantec.com/page.jsp?id=ssl-information-center (besökt 2016-05-28)

Symantec (2012): Internet Security Threat Report 2011 Trends. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf (besökt 2016-05-28)

Want, R. (2009). When Cell Phones Become Computers. *IEEE Pervasive Comput.*, 8(2), pp.2-5.

Watts, S. (2016). Secure authentication is the only solution for vulnerable public wifi. *Computer Fraud & Security*, 2016(1), pp.18-20.