GÖTEBORGS UNIVERSITET

# Kräver ”smarta telefoner” smarta användare?

## En studie av aktuella risker och riskmedvetande hos användare

## Do ”smartphones” require smart users?

**A study of current risks and risk awareness among users**

**JOHN FARGAU PETRINI**
**PER KARLSSON**

**Kandidatuppsats i informatik**

**Rapport nr. 2013:027**
**ISSN: 1651-4769**

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

# Abstrakt

Antalet smarta telefoner är konstant ökande, 2010 såldes globalt ca. 200 miljoner enheter och den siffran förutspås öka till 1 miljard 2016. Den ökade användningen av smarta telefoner medför också många risker. Genom att många smarta telefoner är anslutna till Internet medför detta en väg in för exempelvis dataintrång. Då smarta telefoner är väl representerade i forskning om dess säkerhet lämnar forskning kring dess användande och användares medvetenhet ofta mer att önska, vilket därför är fokus i denna undersökning. Baserat på detta valde vi följande frågeställning som utgångspunkt för vår undersökning: *Påverkar användares riskmedvetenhet deras användande av smarta telefoner sett ur ett säkerhetsperspektiv?*

För att besvara denna frågeställning valde vi att genomföra en netnografisk studie kring två aktuella fall där användare av smarta telefoner utsätts för olika risker genom sitt användande. I vår beskrivning av teori som underlag till undersökningen redovisas en rad olika författares undersökningar och slutsatser kring användares av smarta telefoner riskmedvetenhet. I den grundläggande ansatsen vi utgick ifrån drogs slutsatsen att det fanns ett samband som visade att personer med ingående kunskap i själva verket hade en typ av falsk säkerhet, vilket betyder att de kände sig säkrare än de i praktiken var. I analysen konstaterar vi, baserat på tidigare forskning och vår egen undersökning, att användares riskmedvetenhet påverkar deras användande av smarta telefoner. För att beskriva hur riskmedvetenhet påverkar användningen utvecklade vi olika användarprofiler som adderade ytterligare en faktor till tidigare forskning genom att ta med användares attityder. Baserat på hur de användare som ingick i vår undersökning diskuterade och kommenterade kring fallen utarbetades följande profiler: *"Den självutnämnda experten"*, *"Översittaren"*, *"Den upplyste"* och *"Det ofrivilliga offret"*.



**Nyckelord: Smarta telefoner, riskmedvetenhet, användarfokus**

## Abstract

The number of smartphones are constantly increasing, 2010 approximately 200 million units were sold globally and the figure is predicted to increase to 1 billion in 2016. The increased use of smartphones also carries many risks, for example many smartphones are connected to the Internet. This is a possible way for hackers to gain access to user devices. Smartphones are well represented in research on its safety, while research on its use and users' awareness often leaves more to be desired. That is why the focus of this study is about user awareness. Based on this, we chose the following research question for our investigation: *Do the users risk awareness affect their use of smartphones from a security perspective?*

To answer this question, we chose to implement a netnographic study of two recent cases in which the users of smartphones are exposed to various risks through their use. Our section on earlier research reported a number of different authors investigations and conclusions regarding users risk awareness. The main theory we assumed concluded that there was a link that showed that people with intimate knowledge of threats against smartphones could in fact have a kind of false security, which means that they felt safer than they were in practice. In the analysis we conclude, based on earlier research and through our own study, that users' risk awareness affect their use of smartphones. Further, to describe how risk awareness affects the use of smartphones earlier research inspired us to develop various user profiles that added a new dimension by including users' attitudes. Based on how the users in our study discussed and commented on the cases we created the following profiles: "*The self-proclaimed expert*", "*The bully*", "*The enlightened one*" and "*The involuntary victim*".



**Keywords: Smartphones, risk awareness, user focus**

# Innehåll

# 1. Introduktion

## 1.1 Bakgrund

Antalet smarta telefoner är konstant ökande, 2010 såldes globalt ca. 200 miljoner enheter och den siffran förutspås öka till 1 miljard 2016 (Ridley 2010). En smart telefon är en telefon med mer avancerade funktioner än en "vanlig" telefon. Smarta telefoner är mer lika dagens datorer än gårdagens telefoner då de har många av de funktioner en modern dator har (Wikipedia 2013:c). Den ökade användningen av smarta telefoner medför också många risker, inte bara för den enskilde privatpersonen utan också för företag. Externa minneskort där känslig information lagras kan lätt tappas bort, om en smart telefon säljs utan att minnet raderas eller om den lämnas in på lagning riskeras det att information hamnar i fel händer. Genom att många smarta telefoner är anslutna till Internet medför detta en väg in för exempelvis dataintrång. Om en smart telefon är ansluten via virtuella privata nätverk (VPN) kan detta synliggöra dolda företagsnätverk och på så vis utsätta dessa för risker som hackers, virus och olika spionprogram (Brandel 2010).

I en undersökning som utförts vid Ponemon Institute fick 734 vuxna användare svara på frågor rörande deras användande av smarta telefoner. Av dessa användare var två tredjedelar bekymrade över att bli mål för reklam medan 44 % inte var oroliga för att bli angripna av olika virus eller spionprogram. Mindre än hälften av de som deltog i undersökning uppgav att de använde knapplås eller lösenord för att förhindra att någon tar sig in i telefonen och bara 29 % av de som deltog övervägde att installera ett antivirusskydd eller liknande. Endast 10 % sa att de stänger av möjligheten för andra enheter att hitta deras enhet via bluetooth (Network Security 2011).

Enligt en undersökning CNN nyligen gjort kring antalet smarta telefoner som är infekterade med olika typer av skadlig programvara i olika länder så ligger Kina i topp med 25,5%. Med andra ord har en fjärdedel av den kinesiska användarbasen skadlig programvara i sina smarta telefoner (Inocencio 2013). I ett pressmeddelande från 2013 skriver NQ Mobile att antalet infekterade enheter 2012, enbart på telefoner som använder operativsystemet Android, var över 32,8 miljoner. Detta är i sin tur en ökning med över 200% från 2011 då antalet infekterade enheter var 10,8 miljoner (Titus 2013).

Androulidakis (2012) menar att en av de svagaste länkarna kring mobil säkerhet, bortsett från de tekniska svårigheterna, är användarna själva. Smarta telefoner har blivit en viktig del av vårt

dagliga liv och många användare uppger att deras telefon får dem att känna sig säkrare i vardagen vilket, baserat på ovanstående studier, är en falsk känsla av säkerhet.

### 1.2 Problem

Eftersom dagens smarta telefoner används i många olika sammanhang och under många olika omständigheter förekommer en ny nivå av säkerhetsrisker. Denna nya nivå av säkerhetsrisker förvärras också av den generellt låga nivån av informationsriskmedvetenhet som finns hos många användare. Säkerhetsstandarder kring informationsteknik, exempelvis ISO 27002, omfattar även mobil användning men dessa berör endast tekniska åtgärder såsom säkerhetskopiering, virtuella privata nätverk och kryptering. Lager av olika riktlinjer och strategier kommer att åstadkomma en mycket liten förändring om de inte innehåller element som samtidigt kan öka nivån av medvetenhet hos användare (Allam &Flowerday 2011).

Då smarta telefoner är väl representerade i forskning om dess säkerhet lämnar forskning kring dess användande och användares medvetenhet ofta mer att önska, vilket därför är fokus i denna undersökning.

### 1.3 Syfte och frågeställning

Med vår uppsats vill vi undersöka hur medvetenheten hos användare av smarta telefoner och deras säkerhetstänkande ser ut i dagsläget och formar användares användande. Uppsatsen är tänkt att ligga som grund till vidare forskning inom ämnet men kan även ha en praktisk funktion för användare genom att öka förståelsen och medvetenheten för de olika riskerna som finns. Detta leder således fram till uppsatsens frågeställning:

> *Påverkar användares riskmedvetenhet deras användande av smarta telefoner sett ur ett säkerhetsperspektiv?*

Vi har valt en frågeställning som vid en första anblick verkar simpel då den lättast besvaras med ett “ja” eller “nej”. Vi strävar dock inte efter att besvara denna med ett ja eller nej-svar utan istället med en förklarande analys med bakomliggande faktorer. Anledningen till att vi inte formulerar frågeställningen efter “hur” användares riskmedvetenhet formar deras användande beror på att vi genom denna undersöknings begränsande resurser inte anser oss kunna besvara alla aspekter av en sådan frågeställning. Dock anser vi att genom denna studie kunna besvara om användares riskmedvetenhet påverkar deras användande av smarta telefoner.

För att ge läsarna ett entydigt perspektiv på vad vi i denna uppsats menar med riskmedvetenhet tillhandahåller vi här en definition. Vi placerar in medvetenhet i kontexten av beslutsfattande där den definition av medvetenhet vi har utgått ifrån lyder:

> *Att ta ett medvetet beslut betyder att man tänkt igenom vad beslutet innebär och vilka konsekvenser det kan ha* (Wikipedia 2013:a).

Vi valde denna definition av medvetenhet då den överensstämmer väl med vår egen syn på vad riskmedvetenhet innebär i praktiken. Denna definition applicerar vi i vårt valda sammanhang som graden av förståelse för och kännedom om säkerhetshot mot smarta telefoner.

### 1.4 Avgränsningar

Vi har i denna uppsats valt att begränsa oss till de enskilda användarna. Vi har också valt att avgränsa oss till några av de aktuella hoten som föreligger idag. Med andra ord kommer vår beskrivning av hot mot smarta telefoner att röra de hot som idag ses som aktuella.

### 1.5 Uppsatsen upplägg

Ett vanligt tillvägagångssätt hade exempelvis varit att göra en enkätundersökning med användare för att kartlägga medvetenhet om risker. Dock tror vi att en enkätundersökning inte skulle tillhandahålla så mycket underlag kring användares erfarenheter av att själva blivit utsatta för säkerhetshot. Istället har vi valt att utgå från två fall där användare utsatts för säkerhetshot och observera användares attityder i förhållande till dessa fall. Med andra ord kommer användare identifieras som har erfarenhet av att bli utsatta för mobila säkerhetshot. Genom att granska användares syn på dessa händelser hoppas vi kunna utläsa hur de påverkats i sitt användande. Vi kommer också att beskriva några av de aktuella hot som förekommer idag för klarlägga vad som ligger bakom de fall vi beskriver. Fallen och beskrivningarna av de aktuella hoten ska i slutändan också hjälpa oss att praktiskt illustrera vad användare kan råka ut för och beskriva vikten av att vara medveten om dessa risker. Vår empiriska data inhämtar vi genom en netnografisk studie av olika diskussionsforum på Internet där våra valda fall diskuteras. Dessa blir intressanta för att de visar hur användare diskuterar och agerar kring olika säkerhetshot mot smarta telefoner.

# 2. Teori

I detta avsnitt kommer vi att presentera resultat från tidigare studier där andra forskare undersökt användares medvetenhet kring smarta telefoner och dess säkerhetsaspekter.

### 2.1 Riskmedvetenhet hos användare

Det finns relativt få studier studier om riskmedvetenhet hos användare av smarta telefoner. En jämförelsevis omfattande studie är Androulidakis (2012) som genomförde en undersökning bland 7,172 universitetsstudenter i 17 europeiska länder. Den fundamentala frågan denna studie byggde på var hur säker användare anser att mobil kommunikation är. Majoriteten i undersökningen (36,9%) upplevde kommunikationen måttligt säker, ytterligheterna i denna fråga visade att 13,19% upplevde kommunikationen som säker och 7,82% upplevde kommunikationen som inte alls säker.

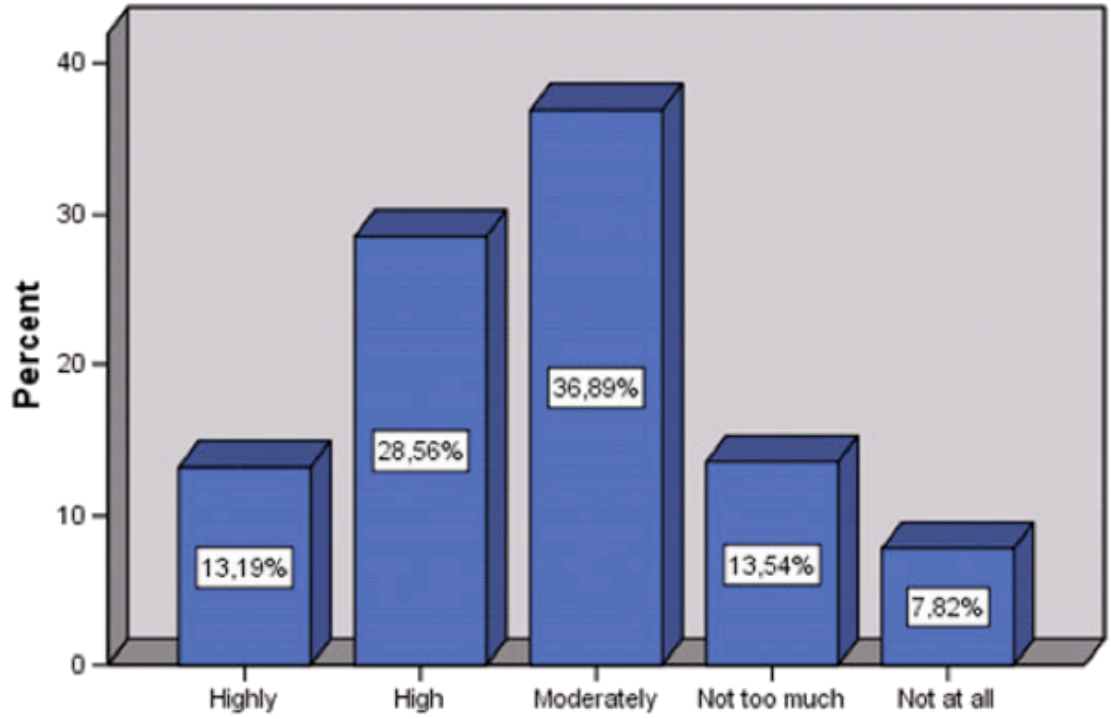


***Diagram 2.1*** *Hur säkra användare i undersökningen anser att mobil kommunikation är där den lodräta skalan visar procentuellt antal och den vågräta visar säkerhetsgraden (Androulidakis 2012, s.29).*

Undersökningen berörde också om studenterna var informerade om inställningar och tekniska funktioner för deras smarta telefoner och hur dessa påverkar säkerheten samt om dessa användare vidtar nödvändiga åtgärder för att minska säkerhetsrisker. Författaren redovisar ett samband mellan en hög känsla av trygghet för mobil kommunikation gentemot hur informerad användaren

var. Även det motsatta förhållandet påvisades genom att användare som inte upplever sig informerade upplever en starkare känsla av otrygghet gentemot mobil kommunikation.

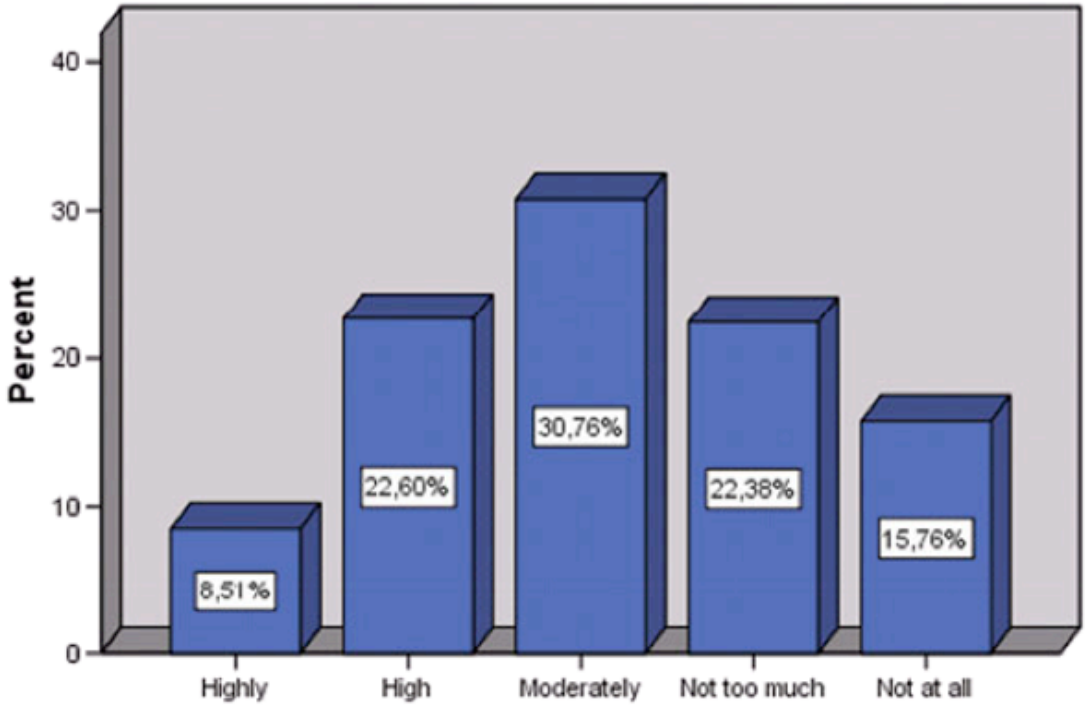


***Diagram 2.2*** *Kunskap om mobila säkerhetsrisker bland användarna där den lodräta visar procentuellt antal och den vågräta visar kunskapen kring säkerhetsrisker (Androulidakis 2012, s. 30).*

Enligt Androulidakis (2012) går det att kategorisera användare i olika väldefinierade grupper baserat på hur säkra de själva upplever att kommunikation med smarta telefoner är. Slutsatsen författaren drog efter att ha kategoriserat in användarna i undersökningen var att det fanns en klar diskrepans mellan upplevd säkerhet och den faktiska säkerheten. Med andra ord fanns det samband kring att användare som kände sig säkra, i praktiken tenderade att vara mindre försiktiga. Detta betydde i realiteten att de var mindre säkra än de kände sig. Författaren beskriver att användare drabbas av kritiska säkerhets- och integritetshot samtidigt som de själva spelar huvudrollen i att skydda sina egna och andras intressen. Eftersom användare idag generellt inte aktivt följer de riktlinjer som finns kring mobil säkerhet borde både teoretiska och praktiska insatser kring medvetenhet sättas in för att ifrågasätta den falska säkerhetskänsla som existerar inom vissa användargrupper idag (Androulidakis 2012).

Chin et al. (2012) beskriver att användare är mer bekymrade för sin integritet när det kommer till användning av smarta telefoner än datorer. Användare är också mer restriktiva när det kommer till att använda olika tjänster på sina telefoner än sina datorer, exempelvis finansiella tjänster eller

integritetskänsliga tjänster. Enligt den studie författarna genomförde bland 60 användare, både kvalitativt och kvantitativt genom intervju och enkät, så är fysisk stöld och förlorad data, bedrägliga applikationer och attacker genom trådlösa nätverk de hot användare av smarta telefoner oroar sig mest för (Chin et al. 2012).

Chin et al. (2012) beskriver också att användare har en annorlunda syn på säkerhet och integritet när det kommer till smarta telefoner jämfört med vanliga datorer. Ett exempel på detta ger författarna genom att många påbörjar en uppgift på sin telefon och sedan slutför uppgiften på sin dator. Detta kan bero på exempelvis svårigheter att skriva på telefonen eller de mobila nätverkens hastighet. Författarna tror också att det finns säkerhetsaspekter som en förklaring till detta. Ett belägg för att säkerhetsaspekterna spelar en roll är att många användare använder sin telefon för att hitta varor de vill köpa men slutför själva köpet på en vanlig dator. Enligt författarna kan en del av den ovan beskrivna problematiken adresseras genom att tillhandahålla gränssnitt som inger ett tryggare intryck på användaren genom att exempelvis försäkra att kreditkortsinformation inte sparas. Androulidakis (2012) studie visar en negativ aspekt av att tillhandahålla trygghets-ingivande gränssnitt genom att det i hans studie framkom att existensen av en ikon som visade att telefonens kryptering stängts av gjorde att användare kände sig mer trygga i sitt användande genom att få återkoppling från sin smarta telefon. Meddelande om att krypteringen blivit inaktiverad kan bero på exempelvis att det nätverk telefonen är ansluten till saknar krypteringen eller har en svag kryptering eller temporär överbelastning. Samma meddelande kan visas när en angripare försöker att initiera vad som kallas för en “man i mitten” attack där angriparen försöker att imitera nätverkets basstation med en falsk som tillsynes är legitim. Angriparen kan därefter kanalisera all kommunikation genom sin egen utrustning och effekt avlyssna den (Androulidakis 2012).

I en ytterligare studie om användandet av antivirus program påvisar Androulidakis & Kandus (2011) att 19% av de 959 deltagarna visste att det existerade sådana program för smarta telefoner men använde medvetet inte dessa medans 44% av deltagarna inte visste huruvida sådana program existerade eller inte. 12,3% av deltagarna använde anti-virus program för sina smarta telefoner. Samma undersökning berörde också om deltagarna förvarade känslig information i sina telefoner. Undersökningen visade att 57% av deltagarna förvarade känslig information i sin telefon. Av detta drog författarna slutsatsen att vi ser våra telefoner som en väldigt personlig ägodel och vi sparar tillika högst personlig och viktig information i våra telefoner. Sådan information bör skyddas men författarnas undersökning visar att användare misslyckas i det. Resultatet av att information stjäls ur smarta telefoner kan således bli förödande för den drabbade. En annan

oroande upptäckt var att 21,6% av de som deltog i undersökningen förvarade okrypterade lösenord i sin telefon, ytterligare 22% förvarade lösenord med någon form av kryptering. Författarna summerar sin undersökning med att konstatera att majoriteten av deltagarna i undersökningen bryr sig om och är oroade gällande dataintrång och att obehöriga kan få tillgång till deras enheter. Dock konstaterar författarna att det inte finns någon kultur kring säkerhet och ingen avancerad teknisk kunskap om deras telefoner. Exempelvis beskriver författarna att en stor del av deltagarna i undersökningen inte kände till att det fanns en ikon som visar telefonens krypteringsstatus. Det var också mycket få deltagare i undersökningen som tog någon form av backup på sina sparade data samt många deltagare som skulle tänka sig att låna ut sin telefon innehållandes känslig information och lösenord till någon annan. Dåligt utformade gränssnitt är ytterligare en faktor som författarna anser vara ett hinder för utvecklingen av någon form av säkerhetskultur bland användare (Androulidakis & Kandus 2011).

### 2.2 Potentiella anledningar till lägre riskmedvetenhet

Androulidakis (2012) beskriver också att ett överdrivet självförtroende eller en stark känsla av trygghet kan leda till en allt för avslappnad inställning till säkerhetsfrågor. Korrelationen i de olika diagram författaren redovisade visade också att de användare som hade en hög uppfattning av säkerhet gentemot mobil kommunikation i praktiken uppvisade sämre säkerhetspraktiker. Det fanns också ett samband mellan den typ av mobila operativsystem användare använde. Beroende på om operativsystemet ansågs avancerat eller inte, upplevde de användare som använde ett avancerat operativsystem sig mer trygga än andra användare med ett mindre avancerat operativsystem (Androulidakis 2012).

Dörflinger et al. (2010) talar också om ett behov av ytterligare säkerhetsåtgärder när det kommer till smarta telefoner eftersom dessa enheter blir mer och mer multifunktionella och är uppkopplade mot skyddade och oskyddade nätverk. Författarna beskriver också att det traditionella skyddet för mobiltelefoner och smarta telefoner, PIN- koden (Personal Idendification Number), inte tillhandahåller tillräckligt skydd när det kommer till lagrad data eftersom den enbart autentiserar användaren till det nätverk han/hon är anknuten till hos en mobiloperatör när den mobila enheten startas. Det finns ingen annan automatiskt spärr aktiverad utan enheten förblir öppen tills den stängs av. Användaren måste göra ett aktivt val för att aktivera andra säkerhets-funktioner. En smart telefons ursprungsinställningar kan ses som osäkra ur ett säkerhets-perspektiv. Författarna hävdar att tekniska lösningar för säkerhet är den slutgiltiga lösningen, men för att sådana lösningar ska kunna utvecklas måste forskare och utvecklare få information från användare för att få en uppfattning om vad användare ser som nödvändiga funktioner. Först då

kan tekniskt lämpliga lösningar tillhandahållas som har en möjlighet att etablera sig på marknaden. Författarna ser ett gap mellan användbarhet och säkerhet. Exempelvis om lösenord blir för komplicerade kanske användare förkastar dessa eftersom det blir för besvärligt att memorera dessa utöver alla andra lösenord som måste memoreras. Med andra ord kan en objektivt förbättrad säkerhet leda till en subjektivt försämrad användbarhet. En sådan situation kan leda till att säkerheten kompromissas genom att användaren exempelvis väljer samma lösenord för flera olika tjänster eller väljer lösenord som är lätta att komma ihåg så som födelsedagar eller namn. Säkerheten kompromissas därför att användaren själv är den svaga länken (Dörflinger et al. 2010).

# 3. Metod

Vår huvudsakliga empiri består av diskussioner på Internet där användare diskuterar risker med användning av smarta telefoner. Vi valde att genomföra en netnografisk studie för möjligheten att observera användarna i deras naturliga miljö. Spårbarhet, då dessa fall vi använt som exempel sträcker sig över en längre period, är en viktig förutsättning för att bilda sig en helhetsuppfattning. Sveningsson et al. (2003) beskriver tre olika sätt att närma sig Internet, som en produkt, process eller metafor. Vi tänker i denna uppsats inte beskriva dessa i närmre detalj utan kan konstatera att vi, författarna, valt att se Internet som en produkt dvs. att "studera mängden av eller innehållet i de meddelanden som användare skickar till varandra i form av text, ljud och bilder" (Sveningsson et al. 2003, s. 59).

## 3.1 Insamlingsmetod

### 3.1.1 Fallstudier

För att besvara frågeställningen valde vi att undersöka två aktuella fall benämnda *"Eurograbber"* och *"Grossen Öland"* vilka beskrivs i detalj i avsnitt 5. Fallstudier är ett bra angreppssätt till studien då vi utifrån ett helhetsperspektiv kan generalisera förhållandena i den studerade målgruppen (Patel et al. 2011). Med andra ord kan fallstudier leda till ett resultat som kan appliceras för användare i andra sammanhang.

### 3.1.2 Netnografisk studie

Vi valde att genomföra en netnografisk studie av två aktuella fall där användare utsatts för hot på grund av sitt användande av smarta telefoner. Likt den etnografiska ansatsen är netnografi ingen metod i sig utan ett samlingsnamn för ett antal olika metoder där den mest vedertagna är deltagande observation och till skillnad från etnografi bedrivs på nätet. Eftersom observation är en empirinära och induktiv metod valde vi således att utgå från tidigare forskningsteorier (Patel & Davidson 2011). Utifrån dessa valde vi sedan att forma egna teorier och profiler kring användares användande av smarta telefoner. Sveningsson et al. (2003) beskriver att målet med etnografisk forskning är att ta reda på de gemensamma värderingar och tankesätt som skapas, inom för uppsatsen aktuella diskussionsforum, och hur dessa påverkar dem. För att få en så bra inblick som möjligt i människors kunskap kring de två fallen valde vi att genomföra observationer för respektive fall där vi undersökte kommentarer och diskussioner på olika forum på Internet kring de två fallen. Vi ville komma åt de människor som blivit berörda av de två fallen för att få ett bredare perspektiv. En observation kan ske på fyra olika sätt, som *deltagande*

*observatör, reporter, wallraffare* eller *spion* (Sveningsson et al. 2003). Vi bestämde oss för att tillämpa spionperspektivet, dvs att observera dolt och ej delta, då detta var angreppssätt som passade studien bäst. Svårigheten med att observera på nätet är att veta var man ska börja. Åtskilliga timmar lades på att flanera, eller "surfa" runt, på nätet för att hitta diskussioner och forumtrådar som berörde de två olika fallen. Svårigheten låg även i att veta vilka beteenden som är representativa för studien (Patel & Davidson. 2011). Kritisk granskning av varje observerat foruminlägg, då detta var vår huvudsakliga källa till empiriskt underlag, var därför något vi hade som förutsättning för att i så stor mån som möjligt kunna härleda dessa till studiens problem och syfte. Vi utgick från sökmotorer och angav sökord relaterade till de två olika fallen. Under processen letade vi efter användare som uttryckte olika åsikter angående problematiken. Vi samlade in en mängd olika diskussioner från forum på internet där fallen var samtalsämnet. Utifrån dessa diskussioner och inlägg valde vi sedan ut citat som vi ansåg vara relevanta och som på något sätt visade eller kommenterade användares användande ur ett säkerhetsperspektiv.

Vid observationerna och insamlingen av den empiriska datan jobbade vi hela tiden tillsammans, dels för att vara så effektiva som möjligt och dels för att tillsammans kunna diskutera relevansen av varje bit insamlad data. Fördelen, enligt Sveningsson et al. (2003), med att analysera asynkron kommunikation som foruminlägg, där det finns tidsstämplar på varje inlägg och möjlighet att kommentera andras inlägg är att vi har möjlighet att röra oss fritt genom tiden. Detta ger oss väldigt goda möjligheter att följa händelseförloppets utveckling och se sammanhanget i materialet.

Vägen fram till vårt resultat föregicks av ett gediget förarbete där vi systematiskt undersökte diskussionsforum med syfte att besvara vår valda frågeställning som ovan beskrivits. Storleken på det material vi gått igenom är svårt att uppskatta men uppskattningsvis så gick vi igenom material i fallet kring Eurograbber som omfattade ett tiotal olika diskussionsforum där exempelvis ett av dessa forum innehöll drygt 50 sidor kommentarer där varje sida innehöll 5 kommentarer. I fallet Grossen Öland gick vi exempelvis igenom ett diskussionsforum med över 150 sidor av kommentarer, där varje sida innehöll 12 kommentarer. Med andra ord fanns det mycket empiriskt material att sortera och stukturera för att slutligen komma fram till de citat som vi valt att ta med i undersökningen. Vår undersökning är således inte baserad på ett fåtal individer utan på ett omfattande empiriskt underlag där vi endast valde de citat som var tydligt knutna till undersökningens syfte.

### 3.2 Analysmetod

Som teoretisk utgångspunkt har vi använt oss av Androulidakis (2012) där han in sin undersökning definierar kategorier för olika typer av användare utifrån deras uppfattning och kunskap om säkerhet för smarta telefoner. Vi gör utifrån Androulidakis gruppering en vidareutveckling utifrån hur användare skapar mening av risker där vi adderar en ytterligare aspekt genom att även studera attityd gentemot de risker som finns. Det konkreta resultatet av denna vidareutveckling blir att vi skapar fyra olika användarprofiler: *"Den självutnämnda experten"*, *"Översittaren"*, *"Den upplyste"* och *"Det* ofrivilliga offret".

### 3.3 Metodkritik

Vi har valt två fall som båda ger rika beskrivningar av konkreta hot som användare av smarta telefoner kan bli utsatta för. Fördelen med att analysera två fall är att det blir möjligt att göra jämförelser och identifiera teman. Dock hade ytterligare fall gett en rikare bild och möjliggjort ytterliggare generaliserbara resultat. Detta var dock inte möjligt då A, tiden för undersökningen var för begränsad. B, det finns inte så många rikt beskrivna fall. C, det fanns mycket foruminlägg kopplade till de två aktuella fallen vilket gjorde det möjligt att följa diskussioner kring användning, säkerhet och risker.

### 3.4 Etik

Vi har i vår underslökning genomfört en netnografisk studie där vi antagit rollen som spion vilket vi anser medför en rad olika etiska aspekter. Enligt Patel & Davidsson (2011) finns det en fyra olika forskningsetiska faktorer som en forskare behöver förhålla sig till, dessa är: *informatikskravet, samtyckeskravet, konfidentialitetskravet* och *nyttjandekravet*.

Alla dessa aspekter är relevanta för vår valda metod, dock ser vi *samtyckeskravet* som det mest aktuella eftersom våra respondenter inte hade möjlighet att bestämma om de ville delta i vår undersöking eller ej (Patel & Davidsson 2011). Men eftersom den information vi inhämtat är skriven på öppna diskussionsforum samt att spionperspektivet är ett etablerat tillvägagångssätt inom netnografin (Svenningsson et al. 2003) ser vi ändå vårt empiriska material som etiskt och moraliskt godkännt. Dock inser vi att det är ett gränsfall gentemot något som skulle kunna benämnas som ett oetiskt tillvägagångssätt.

# 4. Fallbeskrivningar

För att förankra det teoretiska avsnittet till verkligheten kommer vi i följande avsnitt att beskriva två olika fall med kompletterande diskussionsinlägg och upplevelser från faktiska användare. De två fallen, *"Eurograbber"* och *"Grossen Öland"*, kommer översiktligt att beskrivas, hur de gick till och vilka påföljder respektive händelse fick. Diskussionsinläggen är direkt inklippta och oredigerade vilket således i vissa fall föranleder ett relativt grovt språk. Vi har valt att inte censurera dessa då de profiler vi bygger upp i analysen präglas av användarnas attityder. Vi vill därmed be läsaren ha överseende med det stundtals vulgära språket och hänvisningarna till relaterade hemsidor.

## 4.1 Eurograbber

Eurograbber är namnet på en multidimensionell attack som drabbade över 30 000 personer i Europa och där upphovsmännen bakom denna attack kom över drygt 36 miljoner Euros. Genomgående i detta fall var att användare av internetbaserade banktjänster inte hade någon aning om att de enheter de använde var infekterade med skadlig programvara och att pengar stals direkt från deras bankkonton. Eurograbber kan sägas vara en variant av det som benämns som ZITMO eller "Zeus-In-The-Mobile Trojan".

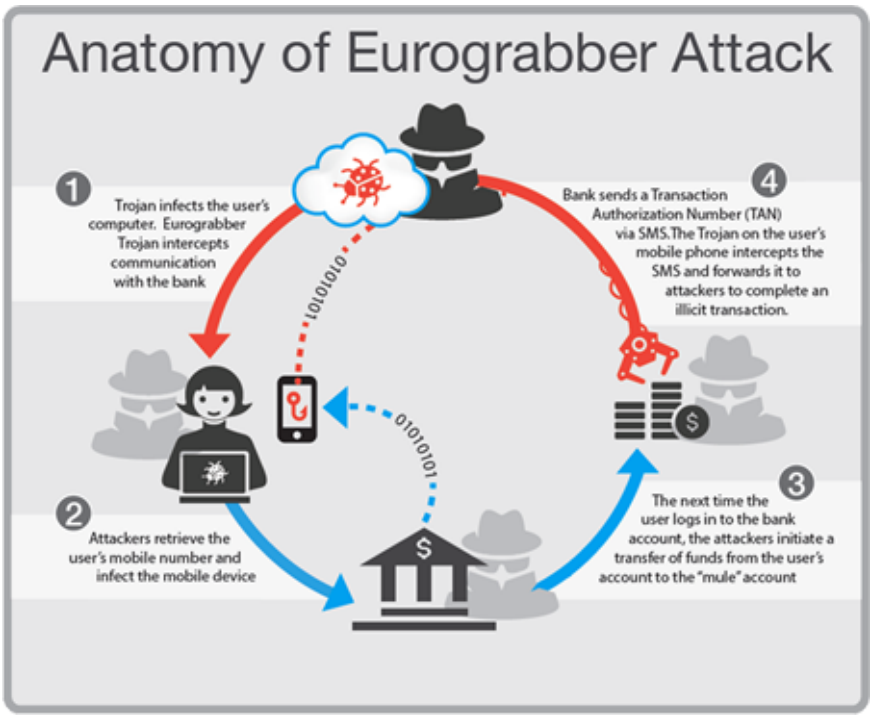


***Fig 3.1*** *Eurograbbers anatomi*[1]

[1] http://www.zonealarm.com/blog/?p=1982

Denna attack bestod av flera olika steg och när både användarens dator och mobila enhet var smittade kunde upphovsmännen bakom attacken helt övervaka och manipulera olika användares internetbaserade banksessioner. Attacken riktade sig mot smarta telefoner med operativsystemen Android och Blackberry för att nå en så stor målgrupp som möjligt av både privata användare och användare med enheter knutna till företag (Kalige & Burkey 2012). Riskmedvetenhet bland användare kom till uttryck i foruminlägg genom diskussioner om hur omfattande man uppfattar att attacken var. Ju mer omfattande attack, desto större anledning för användare att vara försiktiga. I följande konversation diskuterar användare vad som gjorde attacken möjlig:

*Person 1: Pretty impressive. Those malware writers are ingenious :-) you got to admire the effort.*

*Person 2: Biggest Cause is the result of someone clicking on something they should never had clicked on. Guess that a lot of people either never learn or need some serious Education.*

*Person 3: So you, and all those commenters who think only stupid people get infected, run without any anti-virus software, since you are so convinced that your street smarts will prevent any infection? Let us know how that works out for you. (Citat 1)*[2]

Ovanstående konversation är av intresse då det råder delade meningar om vilka användare det egentligen är som drabbas. En användare anser att det till stor del beror på okunskap när användare drabbas av säkerhetshot medans en annan användare invänder att så inte alls behöver vara fallet utan att vem som helst kan drabbas. En annan användare menar att bankerna bär ett tung ansvar kring säkerhetsaspekterna och användaren är ett offer i det hela:

*"Banking is Federally regulated ... but not enough because of the crimes that happen via their vaults, far too often, making victims the big time losers. Banks are PUSHING INTERNET BANKING TO A HIGH DEGREE, and have not really insured that their "banking internet systems" have sufficient integrity to not invite "stage coach internet*

[2] http://arstechnica.com/security/2012/12/sophisticated-botnet-steals-more-than-47m-by-infecting-pcs-and-phones/?comments=1&start=0

*bank robberies" via their implementation of internet banking. If you are going to Push a Product to Market, then you need to insure its safety ... " (Citat 2)*[3]

Ovanstående inlägg är av intresse för att de visar mångfalden kring användarnas reaktioner och syn på vad det var som egentligen hände. Under den senaste tiden i Europa så har de olika finansiella instituten vidtagit åtgärder för att öka säkerheten kring internetbaserade transaktioner. Tidigare behövde användare generellt endast sitt kontonummer och lösenord för att komma åt sina konton via internetbaserade banktjänster. Att bara ha inloggning som består av autentisering i ett steg är en uppenbar säkerhetsrisk eftersom användare ofta väljer svaga lösenord och inte förvarar dessa uppgifter tillräckligt säkert vilket kan leda till att deras konton äventyras. Bankernas lösning på detta problem var att lägga till ett ytterligare steg av autentisering vilket möjliggörs genom att när en användare gör en transaktion skickas ett SMS ut till användarens telefon med ett TAN- nummer vilket står för "Transaction Authentication Number". Transaktionen slutförs genom att användaren anger detta nummer för att godkänna transaktionen (Kalige & Burkey 2012). En användare uttrycker starka känslor om att använda telefonen, enligt användaren en av de mest utsatta artefakterna, vid bankärenden:

*"whoever thought that was a good idea deserves a special hell. sure, lets rely on the most stolen personal object as a security measure, what could possibly go wrong?" (Citat 3)*[4]

Med tanke på att användare i dagens samhälle samlar mer och mer av sin personliga och känsliga information på sin smarta telefon (Androulidakis & Kandus 2011), visar ovanstående en förståelse för problematiken. Som kommentarer på en blogg där ett av bloggens inlägg beskriver händelserna kring Eurograbber läggs snarare skulden på användarnas behov av att använda telefonen till alla vardagliga sysslor inklusive sådana av känslig karaktär:

*"If people weren't desperate to do everything with a mobile phone, this attack couldn't work. Don't use a bank daft enough to send authentication by SMS! Mobile phones are good at, guess what, phone calls and SMS. They take bad photos and they are insecure for finance. They are pretty terrible for everything else. The pity is that the networks*

[3] http://www.zonealarm.com/blog/?p=1982

[4] http://news.slashdot.org/story/12/12/06/061220/how-the-eurograbber-attack-stole-36m-euros

*have convinced a lot of people that they'll cease to exist if they stop using their phone for 5 minutes". (Citat 4)*[5]

En annan användare påpekar att telefonen som en del i säkerhetsarrangemanget brukade vara bra på den tiden telefon och dator var två separata kommunikationskanaler. Med dagens smarta telefoner suddas denna gränsen ut:

*"Actually, using your mobile phone to authenticate a transaction used to be a good idea -- back when phones (and SMS/texting) provided a separate communication channel from the internet, so even if your computer was compromised, you had the chance notice something was amiss. With today's smartphones, there is no real separation anymore, because an attacker just needs to compromise texting and banking apps (or the web browser) on the phone; or on the desktop and the phone, but that is easy because the phone is managed from the desktop" (Citat 5)*[6]

Detta visar på användarnas behov av att förenkla sin vardag och använda telefonen i en mängd olika syften som till viss del äventyrar deras integritet och säkerhet i kombination med att den nya tekniken har suddat ut gränserna mellan datorer och telefoner. Problemet började för de användare som drabbades av Eurograbber när de klickade på en länk som laddade ner denna modifierade trojan på deras dator. Ett exempel på hur detta kunde ske ger Kalige och Burkey (2012) genom att beskriva att upphovsmännen skickade ut skräppost via e-mail med falska länkar. Detta var det första steget i attacken och nästa gång en användare loggade i på sina internetbaserade banktjänster så kände trojanen igen den typen av inloggning vilket utlöste nästa steg i attacken. Trojanen påverkar den pågående internetbaserade banksessionen genom att ge dessa program instruktioner som medför att användaren måste ange sitt telefonnummer. Därefter skickades ett SMS ut till användarens mobila enhet med instruktioner om att genomföra en säkerhetsuppdatering genom att följa de länkar som finns i meddelandet vilket resulterar i att trojanen installeras även i användarens smarta telefon (Kalige & Burkey 2012). I forum-diskussioner tolkas detta beteende som ett uttryck för bristande kritisk medvetenhet bland de användare som blivit lurade att installera trojanen:

---

[5] http://www.zonealarm.com/blog/?p=1982

[6] http://news.slashdot.org/story/12/12/06/061220/how-the-eurograbber-attack-stole-36m-euros

> "*I RTFA (Read The Fucking Article) and while the whole system is quite sophisticated with keylogging trojans etc, in the end it works on the few dumb users who will press an SMS link that says "To install the free cryptographic software on your phone, use this link". Clicking a link on an unsolicited message and especially one that contains the words "Install" and "Free" means you should not own a smartphone, and probably neither a PC with a browser or email client." (Citat 6)*[7]

Nedanstående inlägg är ett svar på ett liknande inlägg som det ovanstående där användaren uttryckte liknande åsikter kring användares okunskap:

> *"Basically, I agree with you. But ask the question: what do you do with the request by Adobe to update Flash Player? If the window that appears is clearly the (well-known, small, red ...) by Adobe?" (Citat 7)*[8]

I kontrast till detta ger det nedanstående inlägget en mer nyanserad bild av det som uttrycks som användares okunskap:

> *"I might qualify for this stupid (dumb user), although I tend to be more paranoid than the average person. My bank does not use this type of stuff but I guess that is not the point. I can see how someone might be "dumb enough". (Citat 8)*[9]

Synen på denna attack är vitt skild angående vad det var som gjorde attacken möjlig att genomföra. En användare ser attacken som en kombination av sofistikerad teknik och användarnas okunskap genom att beskriva det på följande sätt:

> *"Maybe its sophisticated multi-platform attack is a key factor... that, and the obvious careless users who apparently lack any common sense (too bad there is not a "Common Sense" app ;) ). (Citat 9)*[10]

---

[7] http://news.slashdot.org/story/12/12/06/061220/how-the-eurograbber-attack-stole-36m-euros

[8] http://www.spiegel.de/netzwelt/web/eurograbber-trojaner-erbeutet-36-millionen-euro-a-871282.html#spCommentsBoxPager.

[9] http://news.slashdot.org/story/12/12/06/061220/how-the-eurograbber-attack-stole-36m-euros

[10] http://www.techsupportalert.com/freeware-forum/chitchat/10891-meet-eurograbber-botnet-that-stole-36-million-euros.html

Användaren nedan beskriver sitt sätt att skydda sig mot denna typ av attacker:

> *"I never do any banking on-line, and dont have any financial details, account numbers etc, on my computer. To get that information, an arm would need to pop out of the computer, open a drawer some 3 ft away, find the right file, then read the appropriate papers. These hackers might be clever, but I dont think they can manage that!" (Citat 10)*[11]

Dessa inlägg visar att det finns olika grader av förståelse kring hur man ska skydda sig mot denna typ av hot men också att det i vissa fall inte är så lätt att skydda sig. Denna variant av trojanen är speciellt utvecklad för att fånga upp bankens TAN som skickas ut till användarens mobiltelefon. Det SMS som banken skickar ut innehållandes TAN är nyckeln för bankernas tvåstegs-autentisering. Trojanen fångar upp TAN när det skickas ut för att bekräfta sina egna transaktioner som i tysthet sker på användarens bankkonto. Attacken sker helt och hållet i bakgrunden utan användarens vetskap. SMSet med TAN döljs också från användaren eftersom trojanen vidare-befodrar det till servrar som kontrolleras av upphovsmännen till attacken (Kalige & Burkey 2012). Det finns en rad olika kommentarer på olika sidor där fallet Eurograbber beskrivs där många lägger skulden på användarna för att genom okunskap blivit infekterade. Dessa avslutande citat beskriver synen hos majoriteten av de användare som har kommenterat kring fallet:

> *"The eurograbber only have success through the stupidity and gullibility of the user (översatt från Tyska)." (Citat 11)*[12]

> "*The problem always lies between the keyboard and screen (översatt från Tyska)." (Citat 12)*[13]

> *"Hence, human progress basically boils down to this: Our technology can improve, but humans can't! ... most likely, won't!" (Citat 13)*[14]

---

[11] http://www.livingincebuforums.com/ipb/topic/55953-malware-arewere-you-protected-from-eurograbber/

[12] http://www.spiegel.de/netzwelt/web/eurograbber-trojaner-erbeutet-36-millionen-euro-a-871282.html#spCommentsBoxPager

[13] http://www.spiegel.de/netzwelt/web/eurograbber-trojaner-erbeutet-36-millionen-euro-a-871282.html#spCommentsBoxPager.

[14] http://www.zonealarm.com/blog/?p=1982

### 4.2 Grossen Öland

Under sommaren och hösten 2012 genomfördes bedrägeriförsök mot ett stort antal svenska medborgare. Falska fakturor och inbetalningskrav via SMS dök plötsligt upp i svenska hem där de anklagades för att olagligt ha laddat ner porrfilmer utan att betala för dem. Vid efterforskningar kunde det konstateras att företaget bakom bedrägeriet, Grossen Öland AB senare Dquero AB, JeMa, Arcade World, JD Finance och till slut LDB Finans alla ledde till samma person (Forsman 2013). Denne person hävdade att alla som besökt hans sida, wapq.mobi, hade accepterat de avtalsvillkor som satts upp och på det viset gjort sig skyldiga till att betala skadeståndet (Palmkvist 2013). På svenska forum startades diskussioner där folk berättade om hur de och andra drabbats och där en del var oroliga för om de hade drabbats. Citaten som följer visar användare som uttrycker oro till följd av deras eller andras handlingar på nätet:

> *"Är det någon mer som fått brev med krav på skadestånd/ersättning samt hot om polisanmälan efter att ha klickat på en reklam banner på xhamster.com? tydligen kommer bannern bara fram om man ansluter med mobilen, men jag har inte velat testa själv för att slippa frestelsen att klicka vidare." (Citat 14)*[15]

> "*Shit nu blir jag nojig här.. Var inne på xhamster med mobilen och tryckte på nåt med svensk porr.. Hur vet man att man är drabbad har inte fått något än." (Citat 15)*[16]

Ovanstående kommentarer visar på ett beteende som tycks vanligt bland de diskuterande användarna som inte reflekterar kring säkerhetsrisker i förhållande till vad det är man interagerar med på nätet. Forsmans (2013) teori var att användarnas mobila webbläsare hade blivit "kapade". För att lyckas med detta har bedragarna skapat skadliga eller falska webbsidor och reklambanners som senare tillhandahållits hos diverse externa aktörer (Forsman 2012). När användarna i sin tur har klickat på dessa har bedragarnas plan satts i spel. Ett bakomliggande skript har skapat en dold webbläsarsession som i sin tur har slussat användaren vidare till wapq.mobi. Väl där har skripet per automatik accepterat användaravtalet och i sin tur påbörjat strömning eller nedladdning av en slumpmässig film (Forsman 2013). Följande användare beskriver hur de har drabbats och är därmed utsatta för det fallet beskriver:

---

[15] https://www.flashback.org/t1903978

[16] https://www.flashback.org/t1903978p21

*"Jag fick nyss ett SMS ifrån Grossen AB där de vill ha skadestånd för att jag laddat ned porrfilm ifrån piratbay... Jag är bortrest så jag har inte sett till något brev. Vad är detta för jäkla företag egentligen? Och varför har de mitt telefonnummer? Jag har INTE dragit hem något ifrån piratebay med telefonen - bara streamat snusk ifrån ett par vanliga sidor." (Citat 16)*[17]

*"Jag har nu fått tag i "skadeståndskravet". Efter att ha tänkt lite så tror jag att jag vet hur det gått till. Det kan vara så att jag googlat på typ "svensk mobil porr" sen gått in på nån av sidorna jag fått fram (allt detta ifrån min Iphone). Jag vill minnas att en av sidorna frågade om jag var över 18 (fanns väl säkert massa finstilt skit jag inte läste) så jag tryckte "ok". Sedan fanns det filmklipp på sidan man kunde ladda hem. Dock funkade de inte när jag klickade på dem - så jag lämnade sidan snabbt." (Citat 17)*[18]

*"Har även jag fått en faktura på 11250 sek där 11200 avser skadestånd och 50 kronor avser administrativa avgifter. Alla klipp och alla tidpunkter verkar stämma och jag har kommit in på sidan via en banner på slutload.com" (Citat 18)*[19]

*"Jag har en fil på min telefon som hetter det som dom säger att ja har ladat ner. MEN DEN FUNGERAR INTE varför skulle ja betala för nåt som inte går att titta på." (Citat 19)*[20]

Vi har valt ut ovanstående citat för att de konkret beskriver händelseförloppet utifrån de drabbades perspektiv. Som kontrast till detta ifrågasätts det i följande citat hur man i god tro kan hämta upphovsrättsskyddat material utan att betala för det:

*"Hur kan man ladda ned porr från en betalsajt utan att betala? Jag trodde i min enfald att man betalade först med kreditkort eller liknande och sedan fick tillgång till porren? Vad är det för märklig sajt, där man kollar porr och betalar i efterhand?" (Citat 20)*[21]

---

[17] https://www.flashback.org/t1903978p4

[18] https://www.flashback.org/t1903978p34

[19] https://www.flashback.org/t1903978p37

[20] http://www.svenskhandel.se/Varningslistan/Svensk-Handel-Varningslistan/Controleur-Judiciaire

[21] http://sverigesradio.se/sida/artikel.aspx?programid=105&artikel=5487699

För att kunna koppla en användares IP-nummer till ett telefonnummer krävs ett så kallat MSISDN eller Mobile Station International ISDN Number. Ett MSISDN motsvarar ditt personliga telefonnummer och tillhandahålls av din telefonoperatör (Wikipedia 2013:b). Nedanstående användare uttrycker oro för hur enkelt det är för bedragare att komma över personuppgifter när man surfar via sin smarta telefon:

> *"Vad som förvånar mej är att man så lätt kan få tag i ett telefonnummer till en abbonent genom telefonens browser." (Citat 21)*[22]

> *Person 1: Det har varit och är kanske fortfarande så om man surfat att med mobilen på en sida så får hemsidans ägare reda på surfarens telefonnummer. Detta har Post och telestyrelsen kritiserat. Sedan om det är så i detta fallet vet jag inte.*

> *Person 2: Nu har du Person 1 gjort det jobbet som SR borde ha gjort för länge sen. Det är många fler än mig som har undrat över detta och nu äntligen fått ett uttömmande svar. Klart att tänkande läsare ville veta hur skojaren fått tag på "kundernas" adresser. Tyder alltså på att dom inte slog upp godtyckliga adresser i telefonkatalogen, men att "kunderna" faktiskt varit inne på websiten. Dock ett lååångt steg därifrån till att man har berättigade krav att skicka räkning på.*

> *Person 3: Gå in på Facebook, spotify eller Youtube och du lämnar kvar din IP adress till den som vill kidnappa den i ngt obskyrt syfte. (Citat 22)*[23]

De senare citaten beskriver hur användare resonerar kring händelsen och visar hur de är på rätt spår gällande vad som hänt. Det är egentligen bara den enskilde användarens operatör som kan göra denna koppling men de olika operatörerna anlitar så kallade "aggregatörer" för att kunder ska få så bra datatäckning som möjligt och så att intäkter hamnar hos rätt leverantör (Palmkvist 2013). Med andra ord säljer operatörer personuppgifter till diverse olika underleverantörer. Det var genom just en sådan underleverantör bedragarna kom över personliga uppgifter om de olika användarna. Genom att "lura" underleverantörer att personuppgifterna skulle användas till diverse tävlingar kunde bedragarna köpa ut dessa, när de väl kommit över telefonnummer och IP-

[22] http://www.svenskhandel.se/Varningslistan/Svensk-Handel-Varningslistan/Arcade-World-SA/

[23] http://sverigesradio.se/sida/artikel.aspx?programid=105&artikel=5487699

adresser kunde kopplingen till respektive användare enkelt göras via gratistjänster som exempelvis hitta.se (Forsman 2013). Nedan beskrivs användarnas teorier om hur förloppet har skett rent praktiskt:

> *Person 1: Jag är rätt dålig på det tekniska så jag förstår inte till 100% hur det går till, men menar du att operatörerna som levererar mobilt internet, t ex telia, skulle kunna förhindra att det går att få tag på mitt mobiltelefonnummer när jag surfar på min mobiltelefon (i mitt fall en iphone)? Eller ligger problemet i själva telefonen och webläsaren?*
>
> *Person 2: Rent tekniskt går det till så att när du surfar från din mobil så läggs en extra-info till i de data som webbsajten ser, dvs när du passerar din operatörs system. Operatörens system håller reda på att du surfar till megakuk.com, de vet att de har avtal med megakuk.com om åldersverifikation/fakturering, och lägger till infon.*
>
> *Person 3: Tack Person 2 för den mycket pedagogiska förklaringen. Att det är operatörerna som säljer ut sina kunder gör det hela mycket allvarligare. (Citat 23)*[24]

Användarna resonerar sig fram till en förståelse som är nära den faktiska förklaringen. Konversationen visar på hur gemenskapen på ett forum kan verka preventivt syfte då användare konstruktivt resonerar kring händelseförloppet.

[24] https://www.flashback.org/t1903978p56

# 5. Analys

Vi kan genom, både genom den tidigare forskning vi tagit del av, vår undersökning av de två fallen, samt användares diskussioner kring dessa, konkludera att användares riskmedvetenhet i många fall påverkar deras användande. Dock blir det mer komplext att beskriva på vilket sätt riskmedvetenhet påverkar användandet. Vår undersökning kan inte sägas vara talande för alla användare av smarta telefoner men den tillhandahåller vissa mönster som vi anser vara talande för användares beteenden. Dessa mönster ska vi i det följande konkretisera genom att översätta till specifika användarprofiler.

Nedan görs hänvisningar till de konversationer från internetbaserade diskussionsforum där vi hämtat vår empiriska data (se avsnitt 5). Utdragen kommer att grupperas i fyra olika profiler efter användarnas attityder som vi sett som tydligt framträdande i diskussionerna. Profilerna är konkrektiserade användarmönster som till viss del är baserade på och inspirerade av delar av den fakta som ovan presenterats av Androulidakis (2012) och vår egen undersökning. Androulidakis grupperar användare som *highly, high, moderately, not so much* och *not at all* efter deras egen subjektivt upplevda känsla utav hur säker mobil kommunikation är gentemot deras egen kunskap angående säkerhetsaspekter. Vi adderar ytterligare en aspekt till en sådan kategorisering genom att även väva in användarens attityd vilket vi också ser som ett uttryck för användarens medvetenhet ur ett säkerhetsperspektiv. Genom att vi faktiskt indirekt observerar användaren i sin naturliga miljö blir det möjligt att applicera ytterligare dimensioner i kategoriseringen. De profiler vi har utarbetat presenteras nedan:

1. *"Den självutnämnda experten"* är den som ser sig själv som näst intill oantastlig baserat på egna erfarenheter och kunskap.
2. *"Översittaren"* är den som hänsynslöst kör över andra användare utan att tillföra något konkret i diskussionen.
3. *"Den upplyste"* är den som genom andras kunskap ökar sin egen förståelse.
4. *"Det ofrivilliga offret"* är den vars attityd präglas av okunskap. Denne behöver inte vara ett faktiskt offer men innehar en slags offermentalitet.

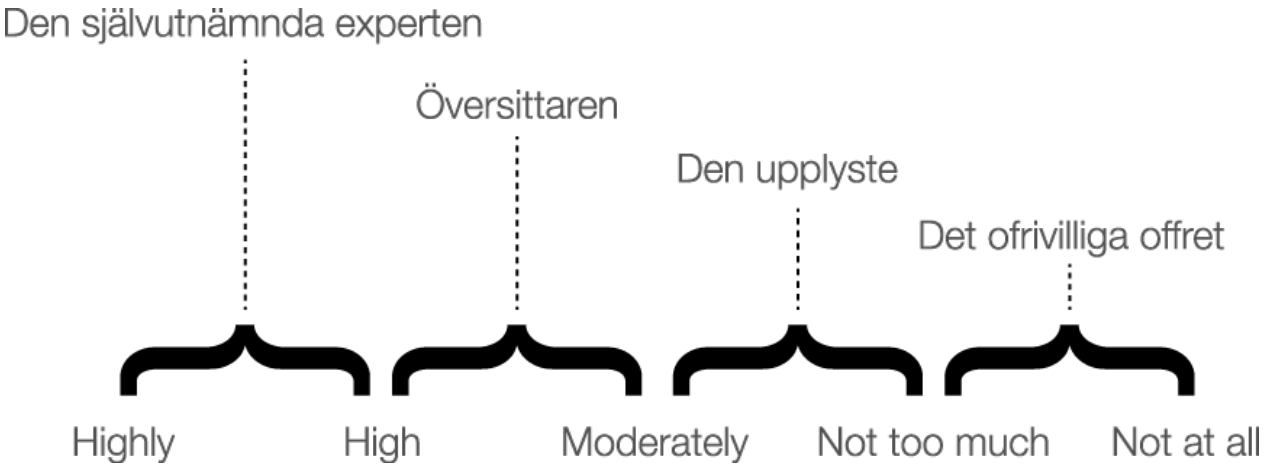


***Fig 5.1*** *Modell över de olika profilerna i relation till Androulidakis (2012) skala: "Highly, High, Moderately, Not too much och Not at all".*

Androulidakis (2012) drog slutsatsen att det fanns ett samband som visade att personer med ingående kunskap i själva verket hade en typ av falsk säkerhet, vilket betyder att de kände sig säkrare än de i praktiken var. Under vår egen undersökning har vi analyserat de olika inläggen vi hittat som på något sätt beskrivit användares sätt att agera gentemot säkerhetshoten. De fyra profilerna vi ovan beskrivit är kontentan av de mönster vi sett hos de inlägg vi analyserat både genom vad användaren faktiskt skriver och vilken attityd användaren har i inlägget till fallet ifråga.

Nedan följer en utförligare presentation av de fyra olika profilerna. De olika fallen innehåller en stor del olika citat vilka passar in på respektive profil, vi har dock i följande presentationer valt ut ett färre antal för att reducera den repetitiva känsla ett större antal kan medföra.

### 5.1 "Den självutnämnda experten"

Denna profil är i grunden inspirerad av de användare som i Androulidakis (2012) undersökning uppgav *"highly"* och *"high"* både angående hur säker de ansåg att mobil kommunikation var och hur ingående deras kunskap om säkerhetshot mot smarta telefoner är. Det finns då en risk att användaren upplever sitt användande som mer säkert än vad det egentligen är. De aspekter som vi själva identifierat och adderat till Androulidakis kategorisering är som föranleder benämningen av denna profil en känsla som vi upplever att dessa användare förmedlar av oövervinnlighet, att stå över "vanliga" användare. *Citat 4* anser vi vara ett tydligt exempel på det som representerar denna profil genom att användaren i fråga exempelvis ser det som självklart att inte använda en bank som verifierar sina transaktioner genom SMS. Även hans syn på att mobiltelefoner bara är bra när det kommer till attringa samtal eller skicka SMS anser vi tyder på att personen i fråga har en bestämd syn på saker och ting och är troligtvis så pass rigid i sin syn att personen inte skulle

kunna se saken på något annat sätt. Personen i *citat 5* har en lite mer ödmjuk framtoning än personen i *citat 4* men vi anser ända att citatet representerar profilen i fråga eftersom det finns samma rigida underton som i *citat 4*. Personen uppvisar kunskap och en övertygelse om förhållandena mellan dagens smarta telefoner och säkerhetsaspekter gällande dess användning. Dessa användare besitter säkert i grunden en ganska stor medvetenhet kring olika säkerhetsrisker för smarta telefoner, men deras betydande kunskap har övergått i något som kan liknas vid arrogans vilket försämrar deras faktiska förmåga att skydda sig mot olika säkerhetsrisker.

### 5.2 "Översittaren"

Denna profil är baserad på de som i Androulidakis undersökning uppgav *"high"* och *"moderately"* både angående hur säker de ansåg att mobil kommunikation var och hur ingående deras kunskap om säkerhetshot mot smarta telefoner är. De aspekter som vi adderar bygger på dessa användares överlägsna attityd. Denna profil anser vi inte som föregående vara byggd på kunskap i samma utsträckning utan denna tillhör något som kan beskrivas som ett mellanting mellan kunskap och okunskap hos användaren. Vi ser användarens nedlåtande attityd som ett uttryck för osäkerhet kombinerat med viss kunskap. Personerna som skrivit *Citat 6* och *12* uppvisar en inställning som dumförklarar alla som som inte har samma syn kring saken i fråga och har ingen förståelse för att andra personer kan ha en annan kunskapsnivå eller infallsvinkel som för dem att se saken i annat ljus. Som citaten visar så finns det en tydlig tendens hos denna profil att skylla på okunskap och dumhet hos andra användare. Dessa användare tillför egentligen inget till de diskussioner de deltar i eftersom de ofta uttrycker sig genom att gå till angrepp mot andra. Det finns även här, lite som i föregående profil, en avsaknad av självinsikt men vi anser att denna självinsikt för profilen snarare bygger på osäkerhet än på överdriven tilltro till sin kunskap.

### 5.3 "Den upplyste"

Denna profil anser vi kunna placeras in i Androulidakis undersökning bland dem som uppgav *"moderately"* och *"not to much"* både angående hur säker de ansåg att mobil kommunikation var och hur ingående deras kunskap om säkerhetshot mot smarta telefoner är. De användare som ingår i denna profil präglas av en mer ödmjuk attityd, exempelvis har dessa användare en förståelse för att man kan begå ett misstag och att det inte är så självklart att handla på "rätt" sätt. Dessa användare besitter inte alltid en djupgående kunskap kring säkerhetshot mot smarta telefoner men vi anser att detta i likhet med Androulidakis (2012) slutsatser gör användarna mer uppmärksamma och vaksamma i allmänhet. *Citat 8* och *9* anser vi vara ett tydliga exempel på hur personer som kan sägas ingå i denna kategori resonerar. Genom att de först uppvisar en förståelse för både själva problematiken i fråga och sedan för att denna problematik kanske inte alls är så

självklar för andra personer. Det finns med andra ord en distans till sin egen kunskap och uppfattning, dessa personer har ett mer öppet sinne och de ser det inte som ett påhopp när andra åsikter tas upp utan bara som att saken kommit i nytt ljus. Detta betyder inte att de nya perspektiven köps med hull och hår, men det finns i alla fall utrymme för reflektion i förhållande till sin subjektiva kunskap. Användarna som ingår i denna profil behöver inte alltid tillföra någon konkret fakta till diskussionen, dock bidrar användarnas ödmjukhet och attityd till att de istället kan upplysa andra användare kring problemet i fråga. Denna attityd fungerar också på motsatt sätt dvs. att användaren själv blir mottaglig och öppen för att vidga sina egna perspektiv.

### 5.4 "Det ofrivilliga offret"

Denna profil anser vi kunna placeras in i Androulidakis undersökning bland dem som uppgav *"not to much"* och *"not at all"* både angående hur säker de ansåg att mobil kommunikation var och hur ingående deras kunskap om säkerhetshot mot smarta telefoner är. Denna sista användarprofil bygger på användare som besitter liten kunskap om säkerhetshot mot smarta telefoner. Androulidakis (2012) beskriver att detta är en grupp som baserat på sin bristande kunskapsnivå är mycket försiktiga i sin användning av smarta telefoner eftersom deras relativt magra kunskap gör dem osäkra. Vi instämmer med denna syn till vis del, dock har vår undersökning visat att denna okunskap också kan leda till misstag med alvarliga konsekvenser. *Citat 15* och *17* anser vi vara tydliga exempel på användare som saknar kunskap kring olika säkerhetsaspekter för smarta telefoner. Personerna bakom citaten beskriver nästan något som vi upplever som chansningar när de väljer vilka sidor de ska besöka. Citaten visar både en person som är relativt likgiltig inför risker och en person som är orolig till följd av sin okunskap. Med andra ord ser vi denna profil som en kategori av användare som kan vara oroliga i antingen situationer där det är obefogat eller befogat alternativt nästan överdrivet nonchalanta. Bristen på kunskap kan som påvisats få olika följder, gemensamt för dessa är dock bristen på kontroll. Vi ser det som att dessa användare har svårt att veta om de utsätter sig för risk eller inte genom sitt användande.

### 5.5 En kontextuell ansats

Under detta avsnitt kommer andra aspekter, vilka tidigare beskrivits i teoriavsnittet, som vi ser påverka användarna att diskuteras.

#### 5.5.1 Användaranpassade gränssnitt

Chin et al. (2012) beskriver att användare har en annan syn på datorer än smarta telefoner. Detta kan bland annat bero på användaren känner sig osäker på telefonens gränssnitt. Genom att tillhandahålla gränssnitt som inger en känsla av trygghet genom att exempelvis försäkra att kreditkortsinformation inte sparas kan denna problematik adresseras. Dock beskriver Androulidakis (2012) nackdelar med att tillhandahålla med trygghetsingivande gränssnitt då dessa kan invagga användaren i någon slags falsk trygghet och därmed öppna upp för attacker som den som benämns som “man i the middle”.

Vi delar Androulidakis (2012) syn i denna fråga då vi ser det som relativt meningslöst att bara tillhandahålla gränssnitt som inger större trygghet eftersom det skulle vara kontraproduktivt ur ett säkerhetsperspektiv och utsätta användare för ytterligare risker. Dock kan det också vara att Chin et al. (2012) menar att sådana gränssnitt ska föregås av att säkerheten faktiskt tryggas genom att man exempelvis ser att kreditkortsinformation inte sparas. Ett sådant perspektiv innebär ju i praktiken att man faktiskt tryggar användandet och mer rättvist kan övertyga fler användare att använda smarta telefoner i fler syften utan samma risk. Vi ser en risk utifrån vår profilering av användare att tillhandahålla mer trygghetsingivande gränssnitt även fast de är underbyggda av säkerhetsåtgärder eftersom vissa av dessa profiler, så som “det ofrivilliga offret”, redan har en så låg kunskapsnivå. Även om vissa tjänster gjordes säkrare så skulle en risk finnas att dessa användare skulle applicera känslan av ökad säkerhet på andra tjänster som inte alls är lika säkra och därmed utsätta sig själva för ytterligare risker.

#### 5.5.2 Perspektiv på säkerhet

Androulidakis & Kandus (2011) summerar sin undersökning med att konstatera att majoriteten av deltagarna i deras undersökningen bryr sig om och är oroade gällande dataintrång och att obehöriga kan få tillgång till deras enheter. Dock konstaterar författarna att det inte finns någon kultur kring säkerhet och att användarna inte har någon teknisk avancerad kunskap om sina telefoner. Dörflinger et al. (2010) talar också om ett behov av ytterligare säkerhetsåtgärder när det kommer till smarta telefoner eftersom dessa enheter blir mer och mer multifunktionella och är uppkopplade mot skyddade och oskyddade nätverk. Författarna beskriver också att det

traditionella skyddet för mobiltelefoner och smarta telefoner, PIN- koden, inte tillhandahåller tillräckligt skydd när det kommer till lagrad data eftersom den bara autentisierar användaren till det nätverk denne är anknuten till hos en mobiloperatör.

För att knyta an till Androulidakis & Kandus (2011) så är det inte förvånande att användare är oroade kring olika säkerhetsaspekter. Grunden till det är som Allam & Flowerday (2011) beskriver att lager av olika riktlinjer och strategier kommer att åstadkomma en mycket liten förändring om de inte innehåller element som samtidigt kan öka nivån av medvetenhet hos användare. Hur man ska gå tillväga för att väcka medvetenhet hos användare är en intressant fråga men inget som vi fördjupat oss i under denna undersökning, dock måste ändå denna tanke väckas. Det som i Androulidakis & Kandus (2011) studie blir mer aktuellt för vår undersökning är att författarna beskriver att det inte finns tillräcklig teknisk kunskap. Men som vi konstaterat, och även Androulidakis (2012) i en senare undersökning, så behöver inte en ökad kunskap innebära en ökad medvetenhet eller en förmåga att undvika säkerhetsrisker.

Det Dörflinger et al. (2010) tar upp är en intressant tanke om något som behöver adresseras rent tekniskt men detta är även något som vi ser skulle kunna begränsas om användare hade en högre riskmedvetenhet. Att endast adressera tekniska aspekter löser inte problematiken i ett mer vidsträckt perspektiv och följande användare summerar detta på ett adekvat sätt:

> *"Hence, human progress basically boils down to this: Our technology can improve, but humans can't! ... most likely, won't!" (Citat 13)*

# 6. Slutsats

För att sammanfatta denna undersökning så behöver en användare som är välinformerad kring olika säkerhetsrisker inte vara mindre säker i verkligheten än denne upplever sig vara. Det finns dock en risk att så är fallet. Detta gäller även användare som inte är välinformerade och inte besitter stor kunskap på så sätt att de då är mer försiktiga. Utan okunskap kan leda till att man utsätter sig själv för risk genom sitt beteende, vilket också illustreras av några av våra citat.

Om vi ska utse en av de profiler vi utarbetat som en att eftersträva så är *"Den upplyste"* den profil där vi ser minst risk för användares användande av smarta telefoner. Eftersom ett visst mått av osäkerhet blandat med ödmjukhet eller viljan att ta till sig ny kunskap, som denna profil karaktäriseras av, är en kombination av egenskaper som leder till tillförsikt och ökad medvetenhet kring olika säkerhetsaspekter vitala för användarnas säkerhet och integritet. Vi kan också konstatera att underlaget för denna profil i Androulidakis (2012) som baseras på användare som i hans undersökning svarat *"moderately"* och *"not to much"*, både angående hur säker de ansåg att mobil kommunikation var och hur ingående deras kunskap om säkerhetshot mot smarta telefoner är, var *"moderately"* det svar flest respondenter angett. Slutsatsen blir därav att en betydande del av användare av smarta telefoner kan sägas tillhöra profilen "Den upplyste", vilket vi ser som ett lovande tecken för den framtida utvecklingen av en ökad riskmedvetenhet. Dock ser vi det som oklart vilken faktor som faktiskt ska utlösa utvecklingen för en ökad riskmedvetenhet.

## 6.1 Vidare forskning

Vi ser att det finns en rad olika uppslag för olika intressanta inriktningar vidare forskning kan ta. Ett sådant uppslag skulle kunna vara att undersöka hur de profiler vi utarbetat påverkar varandra, exempelvis går det att härleda om vissa profiler kan verka kontraproduktivt för en ökad riskmedvetenhet? Ett annat möjligt uppslag skulle kunna vara vilka faktorer som faktiskt kan leda till ökad riskmedvetenhet hos användare av smarta telefoner.

# Litteratur


Allam, S. & Flowerday, S. (2011) An adaptation of awareness boundary model towards smartphone security. *Information Security South Africa (ISSA)*, s. 1-8

Androulidakis, I. I. & Kandus, G. (2011) Mobile phone Security Awareness and Practices of Students in Budapest. *The Sixth International Conference on Digital Telecommunications* (ICDT) April 17-22, s. 18-24

Androulidakis, I. I. (2012) *Mobile Phone Security and Forensics A Practical Approach*. New York: Springer.

Brandel, M. (2010) Smartphones need smart security. *Computerworld*, January 2010, s. 21-23

Chin, E., Porter Felt, A., Sekar, V. & Wagner, D. (2012) Measuring User Confidence in Smartphone Security and Privacy. *Symposium on Usable Privacy and Security (SOUPS)* July 11-13, s. 1-16

Dörflinger, T., Voth, A., Krämer, J. & Fromm, R. (2010) "My smartphone is a safe": the user's point of view regarding novel authentication methods and gradual security levels on smartphones. *Security and Cryptography (SECRYPT)* July 26-28, s.155-164

*Network Security*. (2011) Few aware of Smartphone vulnerability. Issue 4, s. 2, 20.

Patel, R. & Davidson, B. (2011) *Forskningsmetodikens grunder - Att planera, genomföra och rapportera en undersökning*. Lund: Studentlitteratur

Ridley, P. (2010) Outsmarting the smartphone fraudsters. *Network Security, Issue 12*, s. 7-9

Sveningsson, M., Lövheim, M. & Bergquist, M. (2003) *Att fånga nätet - Kvalitativa metoder för Internetforskning*. Lund: Studentlitteratur

# Källor


Forsman, P. (2012) *Falska porrfakturor.*
Tillgänglig:
http://www.internetsweden.se/falska-porrfakturor, [2013-05-06]

Flashback. (2012) *Porrsurfare hängs ut på svensk sida*.
Tillgänglig:
https://www.flashback.org/t1903978, [2013-05-22]

Forsman, P. (2013) *Porrskadeståndskraven - "Behind the scene and under the surface"*
Tillgänglig:
http://www.internetsweden.se/porrskadestandskraven-behind-scene-surface, [2013-05-06]

Gallagher, S. (2012) *Sophisticated botnet steals more than $47M by infecting PCs and phones*.
Tillgänglig:
http://arstechnica.com/security/2012/12/sophisticated-botnet-steals-more-than-47m-by-infecting-pcs-and-phones/?comments=1&start=0, [2013-05-22]

Gizmo's Freeware. (2012) *Meet Eurograbber, the botnet that stole 36 million Euros*.
Tillgänglig:
http://www.techsupportalert.com/freeware-forum/chitchat/10891-meet-eurograbber-botnet-that-stole-36-million-euros.html, [2013-05-22]

Inocencio, R. (2013) *Check your phone: Nations with the most mobile malware*.
Tillgänglig:
http://edition.cnn.com/2013/04/16/business/world-most-mobile-infected-countries/index.html?hpt=hp_c 4, [2013-04-17]

Kalige, E. & Burkey, D. (2012) *A Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware*.
Tillgänglig:
http://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf., [2013-05-22]

Kremp, M. (2012) *"Eurograbber Attack": Handy-Trojaner erbeutet 36 Millionen Euro*.
Tillgänglig:
http://www.spiegel.de/netzwelt/web/eurograbber-trojaner-erbeutet-36-millionen-euro-a-871282.html#spCommentsBoxPager., [2013-05-22]

Lidström, J. (2013) *Ligger bakom en lång rad storskaliga bluffar.*
Tillgänglig:
http://www.svt.se/plus/ligger-bakom-en-lang-rad-storskaliga-bluffar, [2013-05-05]

Living In Cebu Forums. (2012) *How 36 Million Euros was Quietly Stolen via Malware*.
Tillgänglig:
http://www.livingincebuforums.com/ipb/topic/55953-malware-arewere-you-protected-from-eurograbber/, [2013-05-22]

Melin, C. (2013) *Ägaren av porrsajten: "Polisiärt klöddande"*.
Tillgänglig:
http://sverigesradio.se/sida/artikel.aspx?programid=105&artikel=5487699, [2013-05-22]

Palmkvist, J. (2013) *Telia stänger av porrmiljonär.*
Tillgänglig:
http://www.sydsvenskan.se/malmo/telia-stanger-av-porrmiljonar/, [2013-05-06]

Slashdot. (2012) *How the Eurograbber Attack Stole 36M Euros*.
Tillgänglig:
http://news.slashdot.org/story/12/12/06/061220/how-the-eurograbber-attack-stole-36m-euros, [2013-05-22]

Svensk Handel. (2013) *Contrôleur Judiciaire*.
Tillgänglig:
http://www.svenskhandel.se/Varningslistan/Svensk-Handel-Varningslistan/Controleur-Judiciaire, [2013-05-22]

Titus, K. (2013) *Mobile Malware Up 163% in 2012, Getting even Smarter in 2013, According to NQ Mobile*.
Tillgänlig: http://ir.nq.com/phoenix.zhtml?c=243152&p=irol-newsArticle&ID=1806588&highlight=, [2013-04-17]

Wikipedia. (2013:a) *Medvetenhet*.
Tillgänglig:
http://sv.wikipedia.org/wiki/Medvetenhet, [2013-06-03]

Wikipedia. (2013:b) *MSISDN*.
Tillgänglig:
http://en.wikipedia.org/wiki/MSISDN, [2013-05-06]

Wikipedia. (2013:c) *Smartphone*.

Tillgänglig:

http://en.wikipedia.org/wiki/Smartphone, [2013-05-20]

ZoneAlarm. (2012) *How 36 Million Euros was Quietly Stolen via Malware*.

Tillgänglig:

http://www.zonealarm.com/blog/?p=1982, [2013-05-22]