Södertörns högskola | Institutionen för naturvetenskap, miljö & teknik
Kandidatuppsats 15 hp | Medieteknik C | Höstterminen 2014
Programmet för IT, medier och design

Användare, säkerhet och webbläsare

– Ett gränssnittsproblem

Av: Ida Eriksson och Johanna Lundgren
Handledare: Mauri Kaipainen

södertörns högskola
SÖDERTÖRN UNIVERSITY

Abstract

Users, safety and web browsers - an interface problem.

In this paper we describe the problems with today's web browsers within the interface. We are aiming to investigate whether or not the browser interface inhibits users from putting their personal safety settings. A great amount of everyday tasks are performed via the browser, for example banking transactions or uploading images on social media. Therefore the need of a browser user interface that can communicate different security levels and settings so that all users can understand and use the settings that are offered. With the help of theoretical starting points, we seek answers to any shortcomings in the browser interface through user studies. By observing and interviewing our subjects, we concluded that there are flaws in the browser that need to be developed. We want our thesis to open up for discussion in which we want to convey the importance of the users' needs to feel safe in the browser interface to assimilate information about their own safety.

Keywords: web browser, security, integrity, user interface, security settings.

Sammanfattning

I denna uppsats beskrivs gränssnittsproblematiken i dagens webbläsare. Syftet är att undersöka om användargränssnittet i webbläsaren hämmar användarna till att sätta sina individuellt anpassade säkerhetsinställningar. En stor del vardagliga sysslor utförs via webbläsaren, exempelvis hantera bankärenden eller ladda upp bilder på sociala medier. Därför finns det ett behov av att webbläsarens gränssnitt kommunicerar olika säkerhetsnivåer och inställningar så att alla användare kan använda och förstå de inställningar som erbjuds. Med hjälp av teoretiska utgångspunkter söker vi svar på eventuella brister i webbläsaren med hjälp av användarstudier. Genom att observera och intervjua våra försökspersoner kom vi fram till att det finns brister i webbläsaren som behöver utvecklas. Vi vill med vår uppsats öppna upp för en diskussion då vi vill förmedla importensen av att användare behöver känna sig säkra i webbläsarens gränssnitt för att kunna tillgodogöra sig information angående sin egen säkerhet.

Nyckelord: webbläsare, säkerhet, integritet, användargränssnitt, säkerhetsinställningar.

Förord

Vi vill ge ett stort tack till alla våra försökspersoner som ställt upp och möjliggjort datainsamlingen till denna uppsats. Ni vet vilka ni är!

Vi vill även ge ett stort tack till vår handledare, Mauri Kaipainen, för all input och feedback under arbetet med denna uppsats.

Tack.

Ida Eriksson och Johanna Lundgren, Södertörns högskola, Stockholm 2015-01-09.

Begreppsdefinition

Användare

Vi refererar till en användare som en person som dagligen använder sig av en webbläsare för att surfa på internet, det vill säga besöker olika webbplatser från valfri enhet (smartphone, dator etc.).

Användar-/gränssnitt

Ett användargränssnitt är den kontaktyta som kommunicerar med användaren av ett interaktivt system. För att användaren ska kunna nyttja användargränssnittets funktionalitet till fullo krävs det att användargränssnittet möter användaren på ett sådant sätt att användaren förstår vad användargränssnittet förmedlar rent visuellt. Detta sker exempelvis genom att information presenteras i form av bild och text mellan användaren och det interaktiva systemet.

Användbarhet

I denna uppsats kommer vi att prata om begreppet användbarhet. Att något anses användbart innebär bland annat att användaren av ett interaktivt system eller en teknisk artefakt inte behöver anstränga sig för att förstå vad som förväntas av denne för att kunna använda sagda system eller produkt. Det innebär också att systemet ska vara lätt att lära sig och det ska vara säkert att använda. Användare ska kunna utföra det de vill göra på ett effektivt sätt.

Cookies

En cookie (sv: kaka) är en liten textfil som lagras lokalt i din dators minne. Det finns flera olika typer av cookies, bland annat förstapartscookies och tredjepartscookies. En förstapartscookie kan spara information om hur en webbplats ska visas utifrån användarens preferenser, exempelvis gällande språk och upplösning. Cookies från tredjepart kan även lagra information om vilka webbplatser användaren besöker för att samla in underlag gällande webbplatsens trafik. De kan användas för att spara information om användarens beteenden för att begränsa och anpassa innehåll efter denne, exempelvis gällande annonser (Mina Cookies, 2014).

SSL och certifikat

SSL står för Secure Sockets Layer och är ett protokoll som hjälper användare att surfa säkert. Protokollet används för att skydda data vid överföring. Med hjälp av en krypterad kanal skapas en privat kommunikation mellan webbplatsen och användaren i webbläsaren där

utomstående inte ska kunna komma åt personliga uppgifter (Symantec, u.å.). När webbläsaren ansluter till en webbplats som skyddas av SSL begär webbläsaren om att få platsen identifierad. Detta sker med hjälp av ett så kallat certifikat. Man kan antingen skapa ett självsignerat certifikat för sin webbplats eller beställa ett från en utfärdare som gör en kontroll av organisationen/företaget och webbplatsen. Ett SSL-certifikat som har en utfärdare garanterar att webbplatsen är säker. Beroende på vilket certifikat som används kan man se detta i webbläsarens adressfält. Det mest tillförlitliga certifikatet syns med hjälp av en grön låsikon tillsammans med namnet på organisationen/företaget i grönt samt URL som börjar med https:// (Ipeer, 2012).

Surfa inkognitio/privat

Webbläsaren Chrome erbjuder en funktion de benämner som “inkognito”. Inkognitoläget möjliggör att Chrome tillfälligt inte sparar någon information om webbsessionen när användaren surfat färdigt. I praktiken innebär detta att webbhistorik, cookies, lösenord och liknande information inte kommer att sparas i webbläsaren då denne stängts ner (Google, 2014). Andra webbläsare har liknande funktioner men har valt att benämna dem som “surfa privat” eller “InPrivate”.

Innehållsförteckning

1 Inledning

Idag tillbringar svenskarna mycket tid på internet. Hela vårt samhälle börjar närma sig en total uppbyggnad av onlinetjänster. Vardagliga sysslor så som att hantera bankärenden, shoppa online och nätverka via sociala medier är exempel på aktiviteter många dagligen utför. Personlig information är något man delar med sig av, både medvetet eller omedvetet, när man surfar på nätet. Detta oavsett om man shoppar kläder, kontrollerar banksaldot eller surfar på Facebook. Personlig information på nätet kan handla om exempelvis personuppgifter, bankuppgifter, inloggningsuppgifter och lösenord samt datatrafik. Det är också online som vi kan råka ut för bland annat nätfiske, stulna privata uppgifter och kapade konton. Att vara mån om sin personliga integritet handlar i stor utsträckning om att undvika att personlig information hamnar i fel händer. Med hjälp av webbläsarens säkerhetsinställningar kan man påverka spridningen av sin personliga information på nätet. Det finns dock en problematik i användbarheten för att användarna ska förstå och använda sig av funktionerna som erbjuds (Furnell, 2009, s. 176).

I denna uppsats kommer vi att undersöka delar av webbläsaren Chromes gränssnitt. Med hjälp av observationer och intervjuer kartlägger vi delar av webbläsarens användargränssnitt utifrån försökspersonernas egna upplevelser. Det vi vill ta reda på i vår undersökning är hur webbläsarens användargränssnitt möter användaren när det kommer till olika säkerhetsaspekter. Vi tittar på hur gränssnittet visuellt presenterar säkerhetsinformation för användaren och hur användaren uppfattar denna information. Hur tänker användare angående sin säkerhet och vilka behov har de? Utifrån detta drar vi slutsatser och diskuterar vad som finns att förbättra i webbläsarens gränssnitt för att även användare med låg erfarenhet ska kunna nyttja de funktioner webbläsaren erbjuder för att surfa säkrare.

1.1 Syfte

Vi kommer i denna uppsats fokusera på de säkerhetsproblem som är relaterade till webbläsarens inställningar och hur användargränssnittet kommunicerar att en viss säkerhetsnivå erbjuds. Syftet med uppsatsen är att ta reda på hur användare hanterar webbläsarsäkerhet. Vi vill ta reda på om användargränssnitten i dagens webbläsare presenterar säkerhetsinställningar på ett förståeligt sätt.

Målet med denna uppsats är att öppna upp för en diskussion kring hur webbläsare kan erbjuda användare att surfa mer säkert. Vi vill även se i hur hög grad användargränssnittet i Chrome

tillåter användarna att anpassa sina inställningar utifrån sina personliga säkerhetsbehov. Tanken är att resultaten ska ligga till grund för framtida forskning och utveckling inom säkerhet och webbläsare utifrån användarnas behov.

2 Bakgrund

Internet har möjliggjort teknologin som en naturlig del av människors dagliga liv. Detta har skett då teknologin bakom förflyttats från den enbart arbetsrelaterade kontext den var tänkt till från början, till att idag involvera både arbete och privatliv. Utmaningen idag ligger i att skapa kraftfulla applikationer och digitala teknologier som kan användas av människor i alla åldrar oberoende av vilken typ av aktivitet de vill utföra (Blomberg, 2003 s. 965). Det finns dock svårigheter i att designa för flera olika användare som har olika mål och befinner sig i olika kontexter (ibid., s. 975).

I en pilotstudie gällande cookies under höstterminen 2014 upptäckte vi ett problem utanför vårt undersökta område. Sju enklare observationer med sex användare genomfördes i pilotstudien. Uppgiften användarna skulle lösa var att hitta vägen till hur man raderar cookies i sin webbläsare. Alla användare fick samma scenario tilldelat sig. Frustration uppmättes av flera användare och vi insåg då att den största bakomliggande orsaken till detta var hur webbläsaren hämmade deras ansats till att slutföra uppgiften. Problematiken låg i att webbläsarnas användargränssnitt inte levde upp till användarnas förväntningar av navigationen, då flera av dem tappade bort sig på vägen. Detta problem uppstod i de fem mest använda webbläsarna (Chrome, Firefox, Internet Explorer, Safari & Opera) som användes under observationerna.

2.1 Webbläsare och säkerhet

En webbläsare är ett program vars uppgift är att hämta, tolka samt återge information från kodade dokument som lagts upp på en webbserver. Webbläsaren fungerar som kontaktyta mellan användaren och den webbsida denne besöker. Användaren använder webbläsaren, klienten, för att kommunicera med den webbserver som tillhandahåller innehållet på respektive webbplats. Genom ett kommunikationsprotokoll (HTTP) definieras vilken typ av data som ska visas. Data kan bestå av exempelvis text, bild, video och ljud (Niederst Robbins, 2012 s. 23).

I webbläsaren har man möjlighet att genom en inställningspanel skräddarsy sina personliga inställningar för hur webbläsaren ska bete sig och hantera information på de webbplatser man besöker. När man surfar kan man råka ut för en rad olika säkerhetsproblem. Webbläsaren erbjuder många inställningar för att korrigera i hur hög grad man vill skydda sin personliga information. Webbläsarens användargränssnitt kommunicerar även visuellt med användaren gällande säkerhetsinformation utifrån vilken typ av webbplats användaren väljer att surfa på.

3 Aktuell forskningsfront

I dagsläget utvecklas webbläsarna i en otrolig takt, mycket till användarnas fördel när det gäller säkerhet (Wisniewski, 2012). Vi kommer i vår undersökning att förankra vårt arbete i Steven Furnells teorier gällande säkerhet. Problemet är dock att alla funktioner inte kan sättas som standard, det är upp till användarna att bestämma hur säkert de vill surfa (Furnell, 2009, s. 180). Säkerhet är nödvändigt men det är inte något man vill lägga ner tid på. Han menar att det finns en ignorans, ett ointresse av att lära sig om säkerhet då det ofta ses som ett nödvändigt ont. Trots att gemene användare är medveten om att det finns ett behov av att skydda sig förväntar de sig att tekniken ska sköta detta åt dem utan att de behöver engagera sig i större utsträckning (ibid., s.176-177).

Som teoretisk utgångspunkt har vi valt att utgå från Furnell, Jusoh och Katsabas studie (2005). I studien beskriver de ett antal kriterier som bör uppfyllas för att säkerhet ska vara så bekvämt som möjligt för användaren att applicera. De menar att det finns ett problem gällande aspekter utifrån ett användarperspektiv angående säkerhetsanvändning för den slutgiltiga användaren. Säkerhet blir ett hinder om användaren inte förstår hur det faktiskt ska användas. Detta kan verka hämmande då de säkerhetsinställningar som tekniken erbjuder inte används på effektivaste sätt, på grund av användarnas varierande kunskapsnivåer (ibid., s. 27-28). Det är viktigt att säkerhet inte sker på bekostnad av användbarheten. De argumenterar att de förinställda säkerhetsinställningarna i stor mån bör räcka till för att skydda majoriteten av användarna. Samtidigt påpekar de att om dessa var tillräckliga så skulle även möjligheten till att skräddarsy egna inställningar för att höja säkerheten anses som överflödig (Furnell et al., 2005 s. 34). Människor tenderar att undvika säkerhetsinställningar när det är möjligt om de inte förstår hur de ska använda det eller om de känner att det är i vägen. Säkerhetsinställningar måste därför presenteras på ett sådant sätt att den möter användarens behov utan att bli en distraktion (Furnell, 2009 s. 176).

Utmaningen med att skapa *användbar säkerhet* kräver att följande kriterier uppfylls (Furnell et al., 2005 s. 28):

- Säkerhet ska vara *förståelig*. Systemet ska erbjuda användaren meningsfull information som användaren kan ta till sig i de val användaren står inför. Problemet ligger i att tekniskt krångliga begrepp och termer ofta används för att beskriva säkerhetsrelaterade inställningar, vilket exkluderar en stor del av de dagliga användarna. Även den användare som är mindre kunnig bör få hjälp och support för att uppnå den nivå av säkerhet som denne behöver.
- Säkerhet ska vara *lokaliserbar*. Användarna måste kunna hitta de inställningar som de behöver. Om användaren måste spendera för lång tid med att leta efter säkerhetsinställningar finns det stor risk att de ger upp och fortsätter vara oskyddade.
- Säkerhet ska vara *synlig*. Systemet bör visualisera tydligt att säkerhetsfunktioner används. Statusindikatorer bör berätta för användaren vilken typ av säkerhet som för tillfället är applicerad och används. Varningar bör användas för att påminna användaren om att högre säkerhet är efterfrågad.
- Säkerhet ska vara *praktisk.* Att applicera säkerhet får inte ske på bekostnad av systemets effektivitet eller skapa ytterligare problem för användaren som kan uppleva vissa säkerhetsaspekter som påträngande. Det finns en tendens till att stänga av säkerhetsinställningar som upplevs som hinder för bekväm användning av systemet i helhet.

Serrhini och Moussa (2013) har påvisat att det finns en problematik mellan användare och webbläsare när det kommer till säkerhet och webbläsarnas inställningar. Utifrån Furnells forskning har de tagit fram ett verktyg som de kallar för ”Automatic Safe Browser Launcher” (Serrhini & Moussa, s. 159). Detta verktyg ska möjliggöra för användare att få en så säker plattform som möjligt när de surfar på webben utan att de personligen ska behöva ändra på några inställningar i webbläsaren. Verktyget behöver laddas ner till användarens dator för att köras där. Genom ett klick på någon av webbläsarikonerna sätter verktyget igång att automatiskt ställa in den högsta säkerheten i den webbläsare man valt. Man får då reda på vilka inställningar verktyget har ändrat på och om man vill kan man läsa mer om dessa (ibid., s. 166). Ändringarna påverkar bland annat cookies, SSL-inställningar och säkerhetsmeddelanden (ibid., s. 164-165).

Ett annat verktyg som tagits fram är Wahlberg, Paakkola, Weiser, Laakso och Rönings (2014) verktyg som syftar till att visa vad som händer i bakgrunden på webbsidan användaren besöker. Istället för att automatiskt ändra varje inställning i webbläsaren är meningen med deras verktyg att få användaren att bli mer medveten om vad som händer under tiden de surfar (Wahlberg et al., s. 435). Det är mycket som händer i bakgrunden som inte visas för användarna när webbläsare läser in olika hemsidor. Man ser till exempel inte i webbläsaren om hemsidan har sparat data på den lokala datorn eller spårat vilka platser man besökt tidigare med hjälp av cookies (ibid.). Verktyget visar direkt för användarna vilka kopplingar som görs mellan första, andra och tredjepart. Verktyget togs fram med anledning av att det påvisats i tidigare forskning att det finns ett problem mellan kommunikationen av webbläsarens gränssnitt och speciellt icke-tekniska användares uppfattning och förförståelse gällande säkerhet (ibid.). Denna problematik mellan användare och webbläsares gränssnitt var något som Whalen och Inkpen (2005) upptäckte i sin forskning. Säkerhetsinformation uppdagades som något komplicerat för användarna. Det fanns exempelvis en falsk trygghet i att låsikonen förmedlade säkerhet trots att det inte fanns någon förståelse av den korrekta betydelsen. Låsikonen var dock ett sätt för användarna att se vilken webbplats som var säker respektive osäker (ibid, s. 137). Det var enbart två av 16 försökspersoner i undersökningen som hade klickat på låsikonen tidigare för att läsa mer om anslutningen och dess certifikat. Certifikat var sällan förstådda och sällan visade av användarna. Interagerar man inte med låsikonen används den inte till fullo. De menar med detta att även om säkerhetsinformation kan hittas behöver det inte alltid vara till hjälp för användaren. I deras undersökning var dessa certifikat falska och ingen av försökspersonerna upptäckte att webbplatsen bara var en kopia av den riktiga platsen (ibid., s. 142). Även Friedman, Hurleys, Howe, Felten och Nissenbaum tar upp detta i sin forskning (2002). De försökte förstå hur användare uppfattade säkerhet och det visade sig att det inte var många som till fullo förstod vad exempelvis en säker anslutning var. Det behöver inte heller vara någon större skillnad på om man har en högteknologisk bakgrund, kommer från landsbygden eller förorten, säkerhetsinformation kan vara svårt att förstå ändå (ibid. s. 747). Friedman et al. uppmanade att man i framtiden bör fokusera på att designa en lösning som möjliggör en informativ upplevelse för användarna istället för att exempelvis titta på en ikon i tron att något är säkert utan att förstå varför (ibid.). Whalen och Inkpen uttryckte att en av utmaningarna var att få användare att bli mer medvetna om certifikatinformation på ett meningsfullt sätt. Då är det, enligt dem, viktigt att ikonerna standardiseras i samtliga webbläsare för att undvika förvirring för användarna (2005, s. 143).

Säkerhetsrelaterade uppgifter är något som är svårt för gemene användare att hantera (Furnell, 2009 s. 177). Furnell beskriver i sitt arbete från 2009 att de webbläsarversioner som lanserades då blivit ännu mer komplicerade än sina föregångare (ibid., s. 178). Han pekar på att problemet specifikt ligger i de skräddarsydda inställningarna som för Internet Explorer 8 uppgår till 48 alternativ vilket är mer än dubbelt upp mot vad versionen innan hade. Majoriteten av dessa förblir i gränssnittet inte förklarade vilket innebär att användaren själv måste ta reda på vad denne förväntas göra med inställningarna. I arbetet jämför han gränssnittet för inställningspanelen i Internet Explorer 4 med Internet Explorer 8. Syftet med detta är att visa att det mellan de två versionernas gränssnitt inte är någon som lever upp till att vara användbar (ibid.). Trots att teknologin går framåt för att göra webbläsarna säkrare erbjuds inte användarna den hjälp de behöver för att förstå de funktioner som erbjuds. Det är därför enligt honom svårt att argumentera för att webbläsarna med tiden faktiskt förbättrats (ibid.).

4 Problemformulering

Forskningsfrågan bygger på en hypotes vi genererade från vår pilotstudie: att det generellt är svårt för användare att anpassa sin webbläsare ur säkerhetssynpunkt. Både webbplatser och webbläsare bör utgöra en upplevelse tillsammans. Vi anser att dessa två, i stor mån, är separerade från varandra. Idag finns ett stort fokus på att designa webbplatser för en god användarupplevelse, vi tycker att detta även borde involvera webbläsare. Vi anser att även den minst erfarna användaren ska kunna förstå samt våga nyttja de funktioner som erbjuds av webbläsaren för att surfa säkrare.

Verktygen som tagits fram i tidigare forskning (Wahlberg et al., 2014; Serrhini & Moussa, 2013) har varit några försök till att underlätta för användarna genom en automatisering av webbläsarens inställningar, samt ett försök att öka medvetenhet genom att synliggöra det som sker i webbläsarens bakgrund. Dessa verktyg kräver att användaren är medveten om att de finns och att de känner att det finns ett behov av att ladda ner något från tredjepart för att öka sin säkerhet. Redan där uppstår en problematik då vi precis som Furnell (2005) anser att säkerhet inte ska behöva vara något opraktiskt eller svårbegripligt (Furnell et al., s. 28). Det krävs en viss kunskapsnivå för att förstå vad man behöver och vad man ska leta efter utanför webbläsarens egna inställningar.

Furnells forskning och kriterier för användbar säkerhet i webbläsaren är från 2005 och vi ville därför applicera dessa på dagens webbläsare i ett försök att se om det har blivit bättre med tiden. Vilka svårigheter är kvar än idag och hur ser attityden ut bland användare och deras säkerhetsbehov? Den webbläsare som jämfördes i hans senare forskning (2009) är fem år gammal och inte längre aktuell. Denna webbläsare anses inte längre som den mest populära idag. Hans forskning kan bland annat ses som ett underlag för framtida forskning och vi ser att det fortfarande finns liknande problem i förhållandet mellan användare och webbläsarens gränssnitt gällande säkerhetsinställningar. Detta vill vi försöka belysa i vår undersökning som fokuserar på att ta reda på hur användare uppfattar bitar av webbläsarens gränssnittsdesign och deras behov gällande säkerheten i webbläsaren. Vi formulerade utifrån detta följande frågeställning:

- Hur kan webbläsarens användargränssnitt bli bättre på att uppmuntra användare till att surfa säkrare?
- Hur ser användare på sina egna säkerhetsbehov?
- Vilka svårigheter går att identifiera när det kommer till att navigera i webbläsarens säkerhetsfunktioner i användargränssnittet?

5 Metod

Insamling av data har skett genom användarstudier. Först har användarna observerats i sin interaktion med webbläsarens gränssnitt och därefter har de intervjuats gällande sina upplevelser från observationerna. Observation är en metod som lämpar sig väl i en studie som denna, mycket på grund av att man genom observationer kan studera människor gällande vad det är de faktiskt gör. Det människor säger och det de faktiskt gör stämmer inte alltid överens (Blomberg, 2003, s. 969). Därför ansåg vi det lämpligt att kunna stärka observationerna med intervjuer.

För att uppnå en så hög reliabilitet som möjligt har vi, enligt rekommendation av Bell, pilottestat såväl observationsschema som intervjufrågor på en kurskamrat (Bell, 2006 s. 191). Detta möjliggjorde att vi kunde omformulera scenariona samt justera de intervjufrågor som kändes krångligt formulerade eller som var direkt ledande eller värderande. Sådana frågor är något som hon uppmanar till att undvika (ibid., s. 159). För ett validerat resultat har vi hela tiden gått tillbaka till den ursprungliga frågeställningen. Vi har förhållit oss kritiska till att det vi undersöker stämmer överens med frågeställningen, något Thúren påpekar är viktigt för en tillförlitlig undersökning (Thúren, 2007 s. 26). Totalt genomfördes en pilotobservation med

efterföljande intervju samt åtta observationer med efterföljande intervjuer. Resultatet från pilotobservationen användes enbart som underlag för att justera undersökningen inför kommande användarstudier, den utgör alltså ingen del av det insamlade och analyserade dataunderlaget.

Vi lät respondenterna själva välja en tid och plats för intervju och observation för att det skulle passa dem på bästa sätt. För bibehållen kontinuitet vid undersökningen hade vi dock som krav att platsen vi skulle vistas på var ostörd, även detta enligt rekommendation från Bell (Bell, 2006 s. 168). För att få respondenterna så bekväma som möjligt i situationen försökte vi skapa en avslappnad atmosfär genom att bjuda på fika samt ställa triviala frågor innan observationerna med efterföljande intervjuer påbörjades. Vi förklarade i förväg vad som skulle hända under själva observationssituationen så att respondenterna inte skulle känna sig otrygga eller obekväma med att vi spelade in deras svar samt tog tid under respektive scenario (ibid., s. 169). Därför upprättades även ett samtyckeskontrakt (se Bilaga 1) för att vi skulle vara försäkrade om att våra respondenter var väl insatta i vad observationerna och intervjuerna skulle gå ut på. Innan varje användarstudie började vi med att gå igenom kontraktet så att respondenterna skulle vara insatta i sina rättigheter samt våra skyldigheter gentemot dem i hanteringen av deras personliga uppgifter. Då vi utlovade våra försökspersoner anonymitet kommer alla respondenter att refereras till som “Försöksperson 1”, “Försöksperson 2” och så vidare. Anledningen till detta var att vi ville försäkra oss om att de skulle känna sig bekväma med att svara så ärligt och rakt som möjligt.

5.1 Avgränsning

Avgränsningar har gjorts gällande datainsamlingen. Avgränsningen är gjord för att underlätta såväl genomförandet av undersökningen som mätningen av resultatet. Vår ambition var att undersöka de fem största webbläsarna idag. På grund av tidsramarna för uppsatsen insåg vi att detta inte var möjligt att genomföra då det skulle kräva många fler användarstudier och försökspersoner. Vi valde därför att avgränsa oss till den mest använda webbläsaren i dagsläget, som enligt statistik från W3CSchools (2014), är Chrome med en användarandel på cirka 60 procent runt om i världen.

5.2 Urval

Urval av försökspersoner till observation och tillhörande intervju har skett baserat på tillgänglighet utifrån de satta tidsramarna för uppsatsen. Vi gjorde en efterlysning av

försökspersoner som spreds via sociala medier och e-mail (se Bilaga 2). För att få ekologisk validitet har vi försökt sprida ut våra observationer så väl i åldersgrupp som kunskapsnivå. Totalt genomfördes åtta observationer.

5.3 Observation

I vår undersökning har vi använt strukturerade observationer som metod. Detta innebär att vi som observatörer av en situation registrerat information utifrån ett på förhand bestämt fokus (Bell, 2006 s. 191). Observatörer har olika fokus och registrerar olika skeenden på olika sätt, vi gör även privata tolkningar av den information vi tar in. Ensamma observatörer riskerar därför i högre grad att utsättas för bias (ibid, s. 187). Vi har därför på Bells inrådan genomfört varje observation och intervju tillsammans. För att ha samma referensram vid observationerna har vi använt oss av två observationsscheman (se Bilaga 3). Vi hade två olika scheman för Scenario 1 respektive Scenario 2. Det som skiljde de båda schemana åt handlade om hur uppgiften löstes i fallet med Scenario 1 där det fanns ytterligare en liten ruta för att markera hur försökspersonen slutfört uppgiften. Ett "W" innebar att användaren slutfört uppgiften helt med hjälp av webbläsarens gränssnitt medan ett "G" innebar att användaren använt Googles sökmotor för att få fram svaret. För att markera rätt- respektive felklick på vägen till att lösa uppgiften använde vi oss av ett "x" för att markera rättklick respektive "-" för att markera felklick.

5.4 Intervju

Vi valde att hålla semistrukturerade intervjuer vilket innebär att frågorna ställs i en viss ordning och kryssas av från ett i förväg förberett papper (se Bilaga 4) (Bell, 2006 s. 160). Alla citat som direkt använts i uppsatsen har verifierats med respektive respondent för godkännande (Bell, 2006 s. 166).

5.5 Genomförande

I observationerna som genomfördes studerade vi vad som kommuniceras mellan Chromes användargränssnitt och försökspersonerna. Försökspersonerna fick i användarstudierna uppdrag i form av tre scenarion där målet med varje del var att surfa säkrare med de funktioner som erbjuds i Chrome. Syftet med observationerna var att få en bättre förståelse för hur webbläsarens gränssnitt skulle kunna utvecklas i framtiden utifrån användarnas behov. Observationerna avslutades med intervjufrågor för att få fördjupande svar direkt från försökspersonerna. Detta för att ge oss en bättre förståelse för deras upplevelse under användarstudien i mötet med Chromes gränssnitt gällande säkerheten.

Vi utgick, som tidigare nämnt, från fyra kriterier gällande att skapa användbar säkerhet när vi utformade vår undersökning (Furnell et al., 2005 s. 28). Den första punkten handlar om att säkerhet ska vara förståelig. Vi hade som mål att titta på hur försökspersonerna uppfattade begreppen som används för att presentera information i användargränssnittet. Som komplement formulerade vi frågor som handlade om hur försökspersonerna uppfattade dessa begrepp. Den andra punkten handlar om att säkerhet ska vara lokaliserbar. Vi ville i våra scenarion se om det fanns svårigheter i att ändra på specifika inställningar i gränssnittet. Den tredje punkten handlar om att säkerhet ska vara synlig. Vi ville genom observationerna se om det var lätt för försökspersonerna att navigera sig runt i gränssnittet för att hitta olika inställningar. Den fjärde och sista punkten handlar om att säkerhet ska vara praktisk. Det ska vara bekvämt att använda säkerhetsinställningar och dessa ska inte ses som krångliga eller störande för den pågående aktiviteten som utförs av användaren.

Syftet med det första scenariot var att undersöka hur väl informationen i Chromes användargränssnitt kommunicerade med försökspersonerna. Det andra scenariots syfte var att se hur komplicerad aktiviteten var att genomföra i Chromes inställningspanel. Vi ville ta reda på om försökspersonerna uppfattade det som krångligt att ändra i inställningarna och om de var så, varför. Det tredje scenariot hade som syfte att se hur information och aktivitet samverkade med varandra. Vi ville undersöka hur förståelig informationen var på tre olika webbplatser, om den var lokaliserbar, tillräckligt synlig och om den uppfattades som lämplig (störande/icke störande). Webbsidorna som ingick i undersökningen var paypal.com, binero.se samt aftonbladet.se. Anledningen till att vi valde ut just dessa sidor var för att de har olika typer av certifierade anslutningar. Paypal har en så kallad säker anslutning (SSL) med en grön hänglåsikon. Binero har ett certifikat med föråldrade säkerhetsinställningar som symboliseras av ett grått hänglås med en gul varningstriangel. Aftonbladet använder inte SSL på sin vanliga nyhetssida, detta innebär att ikonen som visas symboliseras av ett tomt dokument.

6 Resultat

6.1 Population

Av de observerade försökspersonerna var fyra kvinnor och fyra män i åldrarna 18-58 år. Kunskapsnivån hos försökspersonerna varierade. Tre av försökspersonerna hade ingen

erfarenhet av datorer och dess mjukvara från varken arbetsliv eller utbildning (kurser etc.). Däremot hade de använt datorer privat under minst fem år. Ytterligare tre försökspersoner hade viss erfarenhet genom utbildning på varierande nivå, alltifrån gymnasiala datakurser till högre utbildning inom medieteknik förekom. Två av försökspersonerna hade arbetslivserfarenhet från yrken inom IT. Av de åtta försökspersonerna var det fem som använde Chrome som standardwebbläsare. Sju av åtta försökspersoner använde sin egen privata dator. Den försöksperson som inte använde sin privata dator lånade sin dotters dator under användarstudien.

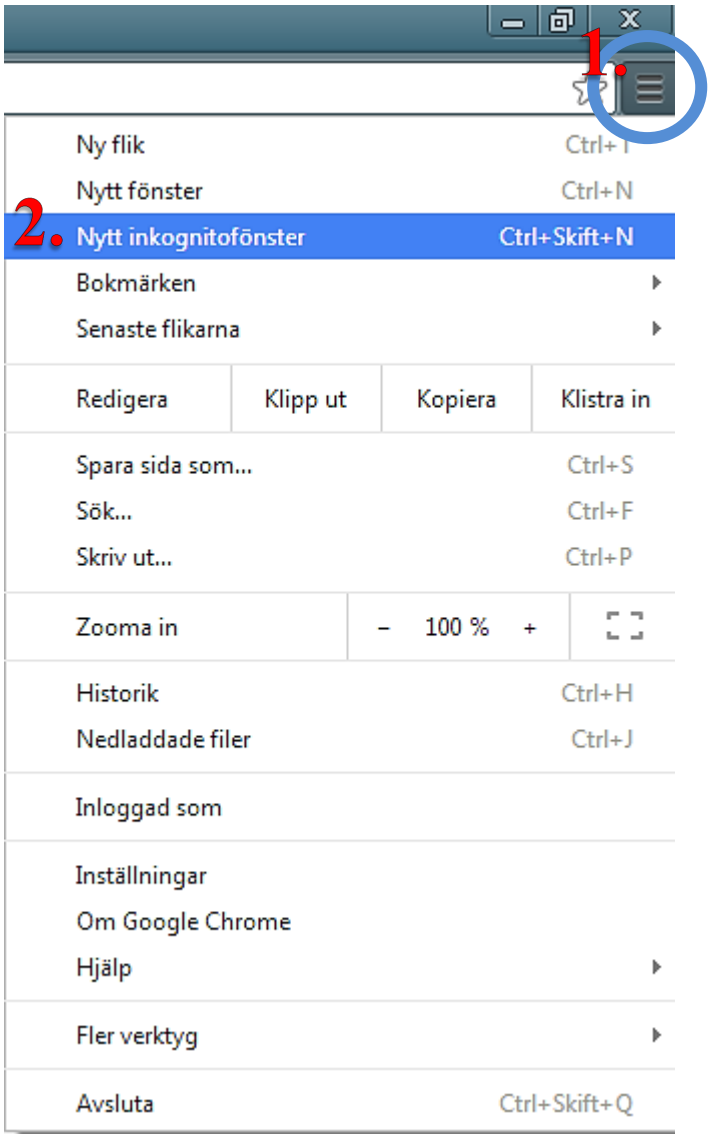
6.2 Användarstudier

Innan användarstudierna påbörjades skrev båda parterna under samtyckeskontraktet. Försökspersonerna fick förklarat att syftet med undersökningen var att undersöka Chromes användbarhet utifrån ett säkerhetsperspektiv. Vi bad försökspersonerna att "tänka högt" under observationerna för att inte missa någon information. För att introducera ämnet började vi med att fråga varje försöksperson vad "surfa säkert" innebar för dem samt vad de själva gör idag för att surfa säkert.

6.2.1 Scenario 1

Scenario 1 gick ut på att försökspersonerna skulle öppna ett nytt inkognitofönster i Chrome där de skulle surfa säkrare. Försökspersonerna fick i förväg inte veta namnet på funktionen, då uppgiften skulle bli för lätt att utföra. De fick istället information om att funktionen är inbyggd i Chrome och att den möjliggör att man tillfälligt surfar med högre säkerhet än i vanligt läge. Vi förmodade att själva funktionen borde varit lätt att använda då den är nåbar på endast två klick. Försökspersonerna fick fritt lösa uppgiften. De försökspersoner som totalt fastnade erbjöds en tid in i observationen att googla fram en lösning om de inte självmant kom fram till att de kunde göra detta.

Scenario 1 gick på totalt två klick för att slutföra uppgiften. Försökspersonen behövde endast öppna *meny* och klicka på fliken *Nytt inkognitofönster* (se Figur 1).



Figur 1. Scenario 1 - vägen till att öppna ett inkognitofönster.

Medelvärdet för totalt antal klick per försöksperson blev fyra. Antal rätta klick var i snitt 2,25 och antal felklick var i snitt 1,75. Totalt tog det i snitt 3:45 minuter per försöksperson att lösa uppgiften. Som kortast tid löstes uppgiften på 0:05 minuter och som längst tid löstes uppgiften på 9:32 minuter. Fem av åtta försökspersoner tog hjälp av Googles sökmotor för att slutföra uppgiften (se Tabell 1).

Sammanställt observationsschema Scenario 1												
Försöks-person	**Antal klick (x = rätt väg, - = fel väg)**										**Hur löstes uppgiften?**	**Tid i minuter**
1	x	x									Webbläsaren	0:05 min
2	-	x	x								Google	8:20 min
3	x	x									Google	2:40 min
4	x	x									Webbläsaren	0:07 min
5	-	-	x	x							Webbläsaren	0:43 min
6	-	x	-	-	-	-	-	x	x		Google	9:32 min
7	x	-	-	x	x						Google	0:47 min
8	-	x	-	-	x	x					Google	5:22 min

Tabell 1. Resultat över scenario 1.

Totalt visste fem av åtta försökspersoner vad inkognitoläge var sedan tidigare och två av åtta hade testat funktionen på en dator innan användarstudien genomfördes. Av de tre försökspersoner som inte visste vad funktionen var sedan tidigare ville två att webbläsaren på något sätt skulle presentera funktionen. Tre av åtta försökspersoner visste med säkerhet vad funktionen gör, således var fem av åtta osäkra eller visste inte hur funktionen fungerar. Tre av åtta upplevde att namnet på funktionen motsvarar det den faktiskt gör. Fem av åtta såg skillnad i gränssnittet på när de surfade inkognito mot när de surfade vanligt. Idag synliggörs inkognitoläget genom en liten illustrerad figur i spionmundering (trenchcoat och mörka solglasögon) uppe i något av webbläsarens hörn samt att färgen på flikfältet diskret ändras (se Figur 2).

Figur 2. Scenario 1 - visuell presentation av inkognitoläge (t.v.) och vanligt läge (t.h.).

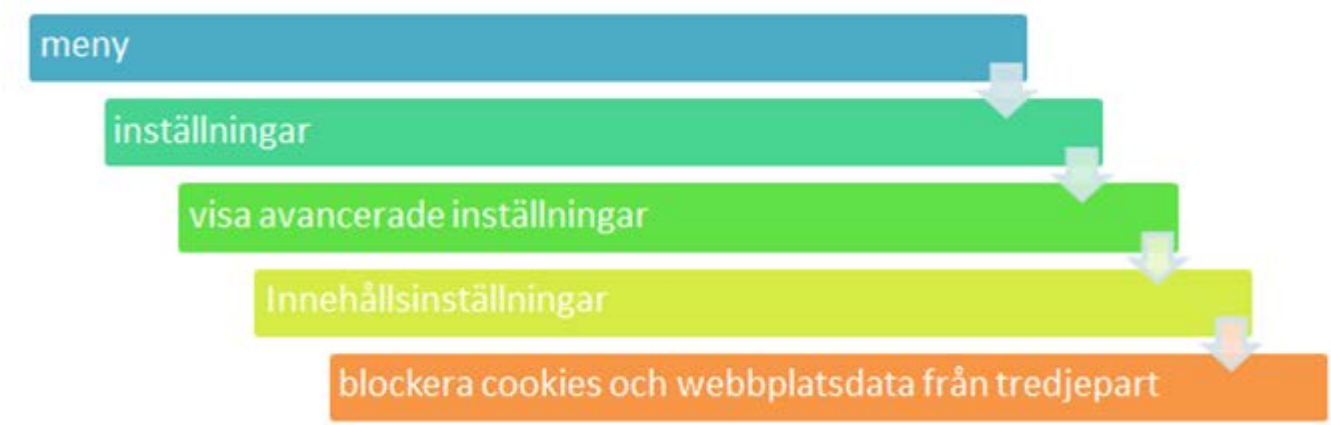
Efter att ha slutfört scenariot ansåg alla försökspersoner att funktionen var lätt att använda. Fem av åtta svarade ja på att de anser att funktionen är relevant och att de kan se att det finns ett behov av den. På frågan om vem man ska skydda information för nämndes anledningar som användning av allmän dator eller familjedator i första hand. I övrigt var

försökspersonerna osäkra eller visste inte vem information bör skyddas från. Exempel som nämndes var hackare, regeringen och utomstående. Förslag som kom upp för att förbättra funktionen var att den borde vara tydligare och mer lättåtkomlig samt att den skulle kunna ingå i en grundinställning då "det är bättre att ta bort det man inte vill ha istället för tvärtom" (Användare 8).

6.2.2 Scenario 2

Uppgiften i Scenario 2 var att gå in i webbläsarens inställningar för att blockera cookies från tredjepart. Scenariot delades upp i två delar. Först fick försökspersonen i uppgift att utföra scenariot på egen hand och därefter gick vi igenom scenariot tillsammans med försökspersonen steg för steg samtidigt som vi ställde frågor om respektive del i gränssnittet.

Scenario 2 krävde totalt fem klick för att slutföra uppgiften. Efter att ha kommit in till säkerhetspanelen via menyn hittade man under *Visa avancerade inställningar* kategorin *Sekretess.* Därefter valde man *Innehållsinställningar* som öppnade en ny ruta med alternativ för bland annat blockering av cookies från tredjepart (se Figur 3).



Figur 3. Scenario 2 - vägen till att blockera tredjepartscookies.

Medelvärdet för totalt antal klick per försöksperson blev 7,87 (se Tabell 2). Antal rätta klick var i snitt 6,12 och antal felklick var i snitt 1,75. Totalt tog det i snitt 3:15 minuter per försöksperson att lösa uppgiften. Som kortast tid löstes uppgiften på 0:29 minuter och som längst tid löstes uppgiften på 7:50 minuter.

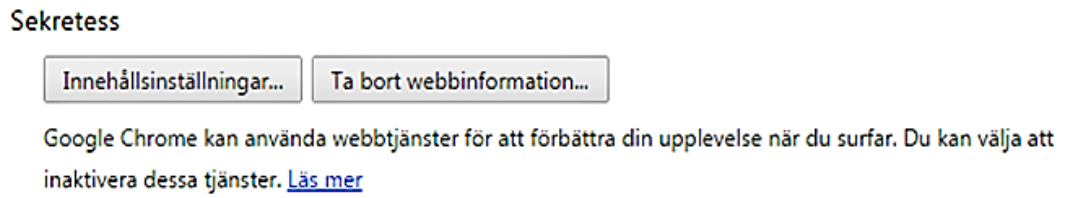
Sammanställt observationsschema Scenario 2																	
Försöks-person	**Antal klick (x = rätt väg, - = fel väg)**																**Tid i minuter**
1	x	x	x	x	x												1:14 min
2	x	x	-	x	x	x											3:33 min
3	x	x	-	-	x	-	-	x	x	-	x	-	-	x	x		7:50 min
4	x	x	x	-	x	x											1:00 min
5	x	x	x	x	x												0:38 min
6	x	x	x	-	-	x	x	x									3:09 min
7	x	x	x	x	x												0:29 min
8	x	x	-	-	x	x	x	-	x	x	x	x	x				7:18 min

Tabell 2. Resultat över Scenario 2.

Fem av åtta förstod vad ikonen för meny innebär (se Figur 4).

Figur 4. Scenario 2 - ikonen för meny innanför den blå cirkeln.

De resterande tre försökspersonerna gissade på att det handlade om någon typ av meny eller ett verktygsfält. Fem av åtta var inte säkra på vad de skulle leta efter i inställningarna för att lösa uppgiften. En av åtta ansåg att stegen för att lösa uppgiften var logiska. Sex av åtta tyckte att terminologin i användargränssnittet på något sätt var svår att förstå. Två av åtta sa sig veta med säkerhet vad *Visa avancerade inställningar* betydde i sammanhanget för scenariot och två av åtta visste inte alls vad det betydde. Resterande försökspersoner (4 av 8) trodde sig veta men var inte helt säkra på innebörden. Ordet *Sekretess* definierade de flesta försökspersoner som att det handlade om säkerhet eller något hemligt och att det som görs inte delas med någon annan. Ingen av försökspersonerna förstod vad rubriken *Innehållsinställningar* i detalj betydde. De flesta uppgav att de antog att det de sökte skulle finnas där (se Figur 5.).



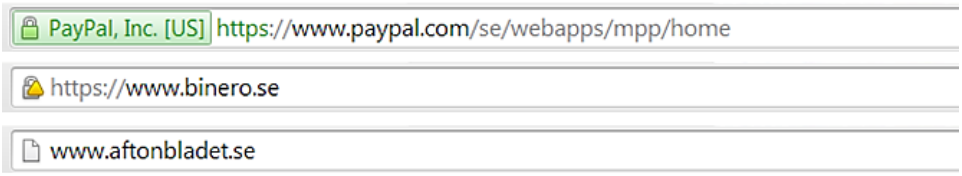
Figur 5. Scenario 2 - knappen *Innehållsinställningar* under *Sekretess*.

Två försökspersoner svarade ja och två försökspersoner svarade nej på frågan om blockering av tredjepartscookies låg på rätt plats. Övriga fyra hade svårt att ha en uppfattning om en bättre plats. En person svarade ja på frågan om huruvida det kändes som att man var på rätt väg efter varje steg. Tre av åtta tyckte att det var lätt att ändra i inställningarna, två av åtta uppfattade det som svårt och övriga tre tyckte varken att det var lätt eller svårt. Fyra svarade ja och fyra svarade nej på huruvida de känner sig säkra med att navigera sig runt i menyn. En person hade sedan tidigare blockerat tredjepartscookies. De som inte hade blockerat tredjepartscookies uppgav att orsaken till detta bland annat var att de inte visste om att de kunde göra det. Två av åtta svarade att gränssnittet delvis berättar om konsekvenserna med de olika funktionerna. En av dessa tyckte att det inte fanns så mycket förklaringar, “på andra webbläsare kanske man kan få hjälp men det finns inte här” (Användare 2). Övriga ansåg att det inte fanns någonting som förmedlar något om vad de olika funktionerna innebär. De förslag som gavs för att förbättra utseendet och terminologin var bland annat att det borde finnas en ”scrollruta” att klicka på med förklarande text (t.ex. vad tredjepartcookies är), och att den kommer upp/försvinner vid klick. Två försökspersoner ansåg att det vore bättre att gränssnittet kunde meddela om konsekvenserna av att markera/avmarkera funktioner som finns bland inställningarna. Andra förslag var att blockering av tredjepartscookies borde finnas bland de primära inställningarna istället för under de avancerade. Ytterligare förslag handlade om att använda mer färg i gränssnittet. Röd text togs upp av två försökspersoner att använda som någon form av varning. Flera försökspersoner ansåg att språket borde förenklas och tydliggöras i gränssnittet, specifikt rubriken *Innehållsinställningar*.

6.2.3 Scenario 3

Det tredje scenariot handlade om att jämföra anslutningen på tre olika webbsidor (Paypal, Binero och Aftonbladet) för att se om det gick att upprätta en säker anslutning (SSL). I adressfältet finns det en typ av ikon (se Figur 6) som säger något om vad som händer och vilken information webbläsaren tar emot från webbservern. Uppgiften försökspersonerna fick

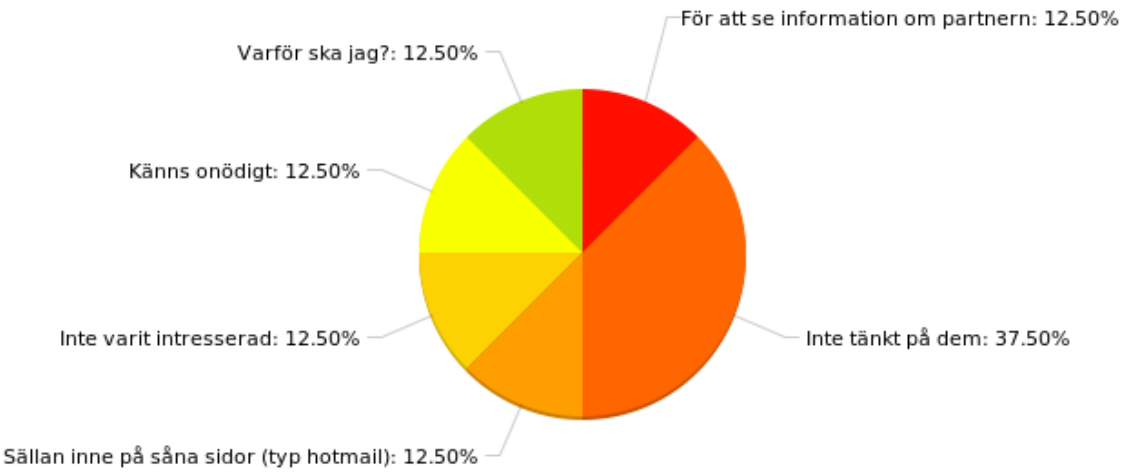
var att berätta hur de uppfattade ikonerna och den information de fick ta del av när de klickade på respektive ikon.



Figur 6. Scenario 3 - ikonerna för de olika webbplatsernas anslutning.

Den gröna låsikonen (Paypal) var bekant för sju av de åtta försökspersonerna. De hade lagt märke till den tidigare och samtliga svarade att ikonen hade något med säkerhet att göra. Detta utifrån deras tolkningar så som: ”en säker webbsida”, ”måste ha access”, ”kryptering”. Däremot var det bara en försöksperson som hade klickat på ikonen tidigare. Den gråa låsikonen med en gul triangel (Binero) var lite svårare att definiera enligt användarna. Endast två av åtta var säkra på dess betydelse. Det var heller inte lika många, fem av åtta, som hade lagt märke till denna i adressfältet och endast en försöksperson hade klickat på den. Dokumentikonen (Aftonbladet) hade återigen sju av åtta försökspersoner lagt märke till. Men endast två var säkra på betydelsen medan andra försökspersoner bland annat svarade att de inte kunde identifiera ikonen med någonting, eller mer än att det kanske är en tidning för att man befann sig på Aftonbladets webbplats. Dock hade två försökspersoner klickat på ikonen. En av dessa två förklarade att han tidigare var nyfiken på vad det var för ikon.

På frågan om varför försökspersonerna tidigare klickat eller inte klickat på någon av ikonerna såg svaren olika ut; allt från att det kändes onödigt till att man ville få mer information (se Figur 7).



Figur 7. Scenario 3 - anledningar till att klicka respektive inte klicka på ikonerna.

När försökspersonerna fick i uppdrag att klicka på ikonerna för att läsa om anslutningen gällande certifikaten på webbplatserna, uppgav fem av åtta att de inte förstod informationen gällande anslutningen på Paypal. Informationen de fick från Binero förstod endast fyra av åtta försökspersoner delvis. En försöksperson uttryckte att informationen från Binero var bättre än den från Paypal, då texten var annorlunda formaterad och skriven på lättare svenska. På Aftonbladet förstod tre av åtta försökspersoner certifikatinformationen, tre av åtta förstod inte och två av åtta var osäkra på om de förstod informationen. Förväntningarna över vilken information som doldes bakom ikonerna realiserades endast för tre av åtta försökspersoner. Det var dessa tre som svarade ja på frågan angående om informationen de fick var den de förväntade sig när de klickade på respektive ikon. Tre av åtta ansåg att informationen de fick var viktig och/eller relevant för dem som användare. Resterande försökspersoner var osäkra på informationens relevans för dem själva som användare.

På frågan angående hur de tolkar informationen från de olika sidorna svarade försökspersonerna bland annat att de kunde se att det handlade om någon form av kryptering. De tolkade Bineros sida som overifierad då den inte hade någon grön färg och de kunde se att den skiljde sig från Paypal på något sätt. Paypal upplevdes generellt av försökspersonerna som säkrast. Hur försökspersonerna upplevde Aftonbladets sida skiljde sig åt. En försöksperson kände sig illa till mods då informationen på sidan uttryckte att den inte var verifierad och försökspersonen upplevde därför webbplatsen som mer otäck än de två övriga. En annan försöksperson uttryckte att han inte förväntade sig någon specifik säkerhet från just Aftonbladet. Två av åtta ansåg att informationen framgått på ett tydligt sätt. Fyra av åtta kände sig säkra angående sin säkerhet utifrån den angivna certifikatinformationen. Tre av åtta kände sig osäkra eller att de helt enkelt inte visste om de kände sig säkrare. En av åtta försökspersoner ansåg att informationen och bland annat terminologin var lättförståelig. Resten ansåg att texten var svår eller att delar av informationen var förståelig medan andra bitar inte sa dem någonting. Fyra av åtta försökspersoner var lite kluvna till att lära sig mer. En försöksperson förklarade att hon ville lära sig mer om säkerhet efter scenariot snarare än den bakomliggande tekniken.

På frågan om de hade några förslag för att förbättra funktionen svarade två försökspersoner att de inte hade några synpunkter för förbättringar. Övriga försökspersoner gav förslag som handlade om att förenkla språket för att få fler, även “otekniska”, att förstå. En önskan gavs

om att implementera text från den webbplats som dyker upp när man trycker på länken *Vad innebär dessa?* direkt i relation till den del i informationsrutan man befinner sig på. De flesta gillade färgkodningen på ikonerna, en försöksperson nämnde att de påminde om trafikljus där grönt är något bra och gult betyder varning.

7 Analys

Som vi tidigare nämnt har vi valt att analysera resultatet med utgångspunkt i de fyra kriterier som Furnell et al. menar ligger till grund för att skapa *användbar säkerhet* (Furnell et al., 2005 s. 28). Vi har därför valt att kategorisera våra resultat utifrån dessa fyra punkter i analysen.

7.1 Förståelig

Enligt den första punkten med kriterier i listan för att skapa användbar säkerhet ska säkerhet presenteras på ett meningsfullt sätt för att vara förståelig. Därför ska, som exempel, tekniskt krångliga begrepp undvikas (Furnell et al., 2005 s. 28).

Generellt ansåg försökspersonerna att terminologin överlag var svårbegriplig. De önskade mer information angående konsekvenser av att avaktivera/aktivera vissa funktioner i säkerhetspanelen. Som exempel fanns det ingen information i Chromes gränssnitt om vad som skulle kunna hända om man blockerade cookies från tredjepart. En försöksperson uttryckte: “Grejen är att... först ska man förstå vad cookies är, sen ska man veta hur man blockerar dem. Hur många som dagligen använder en dator vet det?” (Försöksperson 8). Chrome ger på så sätt inte användarna det de behöver för att förstå terminologin.

Då fem av åtta försökspersoner tog hjälp av Googles sökmotor för att slutföra uppgiften i Scenario 1 kan vi se att funktionen, utifrån användargränssnittets presentation, inte är tillräckligt tydlig för försökspersonerna. Gällande namnet på funktionen var det flera av försökspersonerna som inte förstod vad begreppet syftade på och endast tre av åtta ansåg att termen motsvarade vad funktionen faktiskt gör. Även där indikeras att informationen inte framgår på ett rakt och tydligt sätt till användaren. Furnell diskuterar även rimligheten i att användarna ska ha kunskap om tekniska begrepp (2009 s. 177). Detta kan tyckas som något självklart men så förefaller det inte enligt vår undersökning då flera av försökspersonerna hade problem med begreppen som används i Chromes gränssnitt.

Fem av åtta försökerpersoner upplevde funktionen inkognitoläge som relevant och att de kunde se ett behov av funktionen. Två av tre försökspersoner som inte visste om funktionen sedan tidigare ville att webbläsaren skulle presentera funktionen. Generellt tyckte försökspersonerna att vägen till att lösa uppgiften under Scenario 2 på något sätt var ologisk då sju av åtta försökspersoner stötte på hinder under uppgiftens gång. Alla försökspersoner fastnade på något sätt vid rubriceringen av knappen *Innehållsinställningar* som ingen försöksperson ansåg hjälpte dem för att förstå vad som döljer sig under den. Utifrån detta tolkar vi att Chrome tydligare måste presentera specifika funktioner för användaren för att göra högre säkerhet mer nåbar och synlig.

7.2 Lokaliserbar

Enligt den andra punkten ska säkerhet vara lokaliserbar. Att leta efter säkerhetsinställningar ska inte vara något användarna lägger ner för mycket tid på för att vara skyddade (Furnell et al., 2005 s. 28).

Vi förmodade innan användarstudierna påbörjades att Scenario 1 skulle vara det scenario som gick snabbast för användarna att genomföra. Enligt våra resultat blev det inte så, då genomsnittstiden per försöksperson för att lösa uppgiften låg på 3:45 minuter. Vår hypotes gällande enkelheten i funktionen föll därför och vi insåg att funktionen i enlighet med principen ovan inte alls var så lokaliserbar som vi trott. Även Scenario 2 tog över tre minuter att genomföra. Snittiden för scenariot per försöksperson låg på 3:15 minuter. Att både Scenario 1 och Scenario 2 tog så pass lång tid att genomföra är intressanta aspekter som stärker vår tes att säkerhet i webbläsaren måste presenteras på ett tydligare sätt.

Fem av åtta försökspersoner ansåg att det fanns svårigheter att hitta bland inställningarna under Scenario 2. Detta kan dock bero på att alla inte använder eller aldrig har använt Chrome som webbläsare. De tre användare som använder en annan webbläsare svarade “nej” eller som Försöksperson 2 nämnde, “man får ju peta sig in på de rader man tror sig vara“, på om de tyckte att vägen till att lösa uppgiften var logisk i Chromes gränssnitt. Att det finns framkomlighetsproblem längs vägen som gör att uppgiften blir svår att lösa, är inte till någon fördel för användarna. I enlighet med kriteriet att säkerhet ska vara lokaliserbar för användarna, uppfylls inte detta då användargränssnittet hämmar användarna att hitta rätt. Furnell et al. menar att om användarna inte hittar de inställningar de behöver eller om det tar för lång tid slutar det med att användarna ger upp (Furnell et al., 2005 s. 28).

7.3 Synlig

Den tredje punkten handlar om att säkerhet ska vara synlig och att systemet visuellt bör tydliggöra att en viss typ av säkerhet för tillfället används (Furnell et al., 2005 s. 28).

Det fanns inte något lättillgängligt sätt för försökspersonerna att komma över information angående konsekvenserna av att ändra på inställningarna under *Cookies* utan att behöva besöka en ny webbplats (eller googla). Sju av åtta försökspersoner hade inte blockerat tredjepartscookies tidigare. En av de sju försökspersonerna visste inte att möjligheten fanns. Han förstod inte riktigt varför man skulle behöva göra det eller att det överhuvudtaget gick att blockera dessa. Då blockering av tredjepartscookies inte upplevdes som synlig, då det är en lång väg att gå, blev inställningen automatiskt inte lokaliserbar eller förståelig. Furnell menar att säkerhet måste presenteras på ett sätt som inte distraherar användaren. Detta då säkerhet kan komma att bli ett hinder om användaren inte förstår hur den ska appliceras. Därför måste säkerhet implementeras på ett sådant sätt att den tar hänsyn till alla användares varierande kunskapsnivåer (Furnell et al., 2005 s. 27-28; Furnell, 2009 s. 176).

Fem försökspersoner svarade ja och tre svarade nej på om de ser skillnad på när de surfar i inkognitoläge mot när de surfar vanligt. Vi anser utifrån detta att det finns potential att än mer visuellt tydliggöra inkognitoläge i gränssnittet när det används.

I Scenario 3 fanns tre ikoner med information som försökspersonerna fick analysera och diskutera (grön/grå låsikon samt dokumentikonen). De flesta av försökspersonerna hade inte klickat på ikonerna tidigare. Orsakerna var bland annat att de inte visste att man kunde klicka på dem och att det fanns ett ointresse. Enligt Furnell skulle detta helt enkelt bero på okunskap hos användarna och därför är det extra viktigt att webbläsaren hjälper användaren att förstå skillnad på säkra respektive osäkra sidor utan att terminologin eller osynlighet hämmar inlärningen för användarna (ibid.).

7.4 Praktisk

Det sista och fjärde kriteriet handlar om att säkerhet ska vara praktisk, med andra ord får säkerhet aldrig komma i vägen för systemets effektivitet eller skapa problem för användaren (Furnell et al., 2005 s. 28). Som en försöksperson uttryckte det: “Hur ska man kunna surfa helt vanligt och tänka på allt som kan hända?” (Försöksperson 3).

Vi kunde i vårt resultat inte hitta någonting som antydde att försökspersonerna upplevde att säkerhetsindikatorerna var påträngande, snarare tvärtom. Vi tror dock att säkerhet kan bli opraktiskt när det är för osynligt. Om det inte dyker upp någonting som får användaren att tänka efter gällande sin säkerhet riskerar många att förbli oskyddade. Vi tror på att skapa medvetenhet utan att det ska vara störande.

Ikonerna i Scenario 3 har tidigare inte uppmuntrat försökspersonerna till att klicka på dem, då flera av dem konstaterat att de inte visste att man kunde göra det. Många av försökspersonerna visste inte riktigt vilken typ av information de förväntade sig att få ta del av och certifikat vad således inte heller något de förstod särskilt mycket av. Den information angående certifikat och dess SSL-anslutning i form av ikoner och text, tenderar i vår undersökning vara otillräcklig för att användare ska uppfatta informationen som meningsfull. Whalen och Inkpen observerade redan 2005 i sin undersökning att detta var ett problem och vi ser tendenser i vår undersökning att inte mycket har förändrats (Whalen & Inkpen, s. 143). Ikonerna används inte i den utsträckning som är tänkt. Genom att vara någorlunda osynliga är de heller inte praktiska för användarna, då informationen inte kommer fram trots vikten av att förstå att en hemsida är säker eller osäker.

8 Slutsatser

Genom vår frågeställning ville vi söka svar på hur webbläsarens användargränssnitt kan bli bättre på att uppmuntra användaren till att surfa säkrare, hur användare ser på sina egna säkerhetsbehov samt vilka svårigheter som är identifierbara gällande navigationen i webbläsarens säkerhetsfunktioner i användargränssnittet.

8.1 Hur kan webbläsarens användargränssnitt bli bättre på att uppmuntra användare till att surfa säkrare?

Terminologin bör bli lättare att förstå, speciellt i säkerhetspanelen där många begrepp upplevs som svårbegripliga. Användbarheten sjunker då användarna inte kan få för dem meningsfull information om vad de kan tillåtas göra i användargränssnittet. Det är inte meningen att användarna ska sitta och gissa vad de olika begreppen betyder. Därför bör hjälp finnas lättillgänglig för användarna, men också att begreppen standardiseras. Vi anser att försökspersonernas designförslag gällande en ”scrollruta” med förklarande text och mer färg i gränssnittet skulle kunna implementeras för att tydliggöra säkerhetsinformation.

Det skulle även vara bra om man tydliggjorde säkerhetsfunktioner för användarna, som att exempelvis synliggöra att det finns en interaktion med ikonerna gällande certifikatinformationen. Om en funktion ska användas som det är tänkt är det viktigt att hela funktionen fungerar utan hinder och att interaktionen är förståelig. Att i gränssnittet tydligare visuellt presenterar att specifika funktioner används och är aktiverade, exempelvis inkognitoläget, skulle kunna medvetandegöra användarna gällande säkerhetstänk. En lösning skulle också kunna vara att högre säkerhet är inställt i webbläsaren som standard.

8.2 Hur ser användarna på sina egna säkerhetsbehov?

Vi kunde se att det fanns en viss okunskap och ett ointresse gällande säkerhet. Vi kunde även bekräfta det Furnell sett gällande fördomen att säkerhet upplevs som krångligt (Furnell, 2009 s. 176-177). Användarna förstod inte att certifikat är viktigt för deras egen säkerhet, gällande personliga uppgifter som exempel. Vad detta beror på och vad man kan göra åt det är dock inget vi har fått svar på.

8.3 Vilka svårigheter går att identifiera när det kommer till att navigera i webbläsarens säkerhetsfunktioner i användargränssnittet?

Vi såg indikationer på att det fanns en allmän uppfattning om att det var krångligt att ändra i sin webbläsares inställningar. Gränssnittet i en webbläsares inställningspanel bör vara lättnavigerat och överskådligt, så att gemene användare känner sig bekväm med att sätta sina individuellt anpassade säkerhetsinställningar. Vi anser det viktigt att användare ska kunna hitta rätt på några få klick utan att bli förvirrade på vägen i säkerhetspanelen. Navigationen ska inte behöva bli så pass djup att användare blir förvirrade över var de befinner sig bland svåra begrepp och navigationsnivåer. Oavsett kunskapsnivå ska man ha möjligheten att hitta det man letar efter. Detta blir extra tydligt då gränssnittet hämmar användbarheten istället för att uppmuntra till en naturlig interaktion, där användaren samspelar med gränssnittet och intuitivt erbjuds lösningar.

9 Diskussion

Vi tycker att man aldrig ska behöva kompromissa med sin egen säkerhet online på grund av bristande kunskap i hanteringen av webbläsarens inställningar. Därför måste det öppnas upp för en diskussion som lyfter ämnet och får utvecklarna samt användarna av webbläsarna att reagera på de säkerhetsrelaterade problem som finns idag. Vi anser att alla användare ska

kunna känna sig säkra med att navigera sig runt i de olika inställningarna för att själva kunna fatta egna beslut utifrån sina personliga säkerhetsbehov.

Tekniken erbjuder användarna funktioner för att höja sin egen säkerhet, men det det är upp till respektive användare att välja om de ska göra detta eller inte. Därför måste webbläsarna uppmuntra detta och visa de funktioner som finns. Säkerhet ska inte vara något som ses som ett nödvändigt ont, säkerhet bör vara något som är självklart och lätt att använda. Säkerhetsinställningar ska inte vara skrymmande men ändå lättillgängliga. Därför är det är viktigt att säkerhet inte sker på bekostnad av användbarheten i webbläsaren. Det finns tendenser som vi kan se utifrån vår undersökning som tyder på att användarna struntar i säkerhet om terminologin är svårbegriplig. Detta är även något Furnell (2005; 2009) problematiserat kring i sin forskning. Vi tror att det handlar om användarnas attityd till säkerhet. Frågan som fortfarande finns kvar att besvara handlar om vad som är orsak till denna ignorans. Det fanns till exempel ett ointresse gällande ikonerna och certifikatinformation i Scenario 3. Vi har dock svårt att egentligen förstå varför detta skulle vara ointressant. Enligt vår uppfattning är det idag många som använder exempelvis någon internetbank som kräver en hög säkerhet för sina användare. Då är det viktigt att kunna se att webbplatsen skyddas med någon form av kryptering och att platsens identitet är verifierad för att man ska förstå att ens personliga information och kontouppgifter är så säkra som de kan bli. Detsamma gäller för sociala medier som exempelvis Facebook där bilder, platsangivelser på var man befinner sig och adressuppgifter laddas upp. Detta ointresse för certifikat bekräftades redan 2005 i Whalen och Inkpens undersökning (Whalen & Inkpen., s. 142). Arbetet med hur man kan få användare att bli mer medvetna om certifikatinformation, att göra den informationen meningsfull samt öka tillgängligheten för de som vill ha informationen är idag, tio år senare, fortfarande utmaningar som kvarstår.

De tredjepartsverktyg som vi tidigare nämnt under kapitlet *Aktuell forskningsfront,* hade som mål att hjälpa användare att surfa säkrare. Detta genom att antingen automatiskt ställa in de högsta säkerhetsinställningarna i den webbläsare man valt, eller försöka öka medvetenhet genom att visa vad som sker i bakgrunden (i webbläsaren) när man surfar. Dessvärre tror vi att det krävs en viss nivå av kunskap för att man som användare ska känna ett behov av att ladda ner ett tillägg från tredjepart. Man ska veta vad man har för säkerhetsbehov och hur man kan göra något åt det. Det kan också vara problematiskt att hitta dessa verktyg om man inte

vet var man ska leta någonstans. Om de generella användarna, i likhet med våra försökspersoner, besitter en viss okunskap och ointresse, tenderar nedladdning av tredjepartstillägg att falla redan i steg ett. Detta innebär att dessa förblir okända för användarna. Vi tror dock att man kan implementera liknande funktioner direkt i webbläsarna som en grundläggande funktion, men som också går att upptäckas av användarna på ett lättillgängligt sätt utan implikationer.

Vi har svårt att se om webbläsarna blivit bättre med tiden. Vi ser snarare att vissa funktioner blivit bättre, men att det fortfarande återstår problem med bland annat terminologin, navigationsnivåerna och presentationen av funktionerna. Däremot ser vi att säkerhet har blivit mer aktuellt med tiden och att webbläsarutvecklarna idag tävlar om vilken klient som erbjuder den bästa säkerheten för användarna (Wisniewski, 2012). Om det fortsätter utvecklas åt detta håll tror vi, med största sannolikhet, att webbläsarna bara kommer att bli bättre och bättre med tiden - till användarnas fördel.

9.1 Metodkritik

Vi valde att kombinera två ganska krävande metoder i vår undersökning. Både observation och intervju är metoder som samlar in och mäter kvalitativa datavärden. Nackdelen med detta är att vi i vår undersökning inte har fått in något kvantitativt dataunderlag att dra bredare slutsatser från. Det dataunderlag som är genererat utgår endast från åtta försökspersoner vilket gör det svårt att se tydliga generella mönster som kan appliceras allmänt för en bredare grupp användare än den undersökta. Vi valde att avgränsa oss till att undersöka endast en av dagens alla webbläsare. Hade vi valt att undersöka flera webbläsare hade vi kunnat hitta fler relevanta kopplingar och haft underlag för att jämföra de olika gränssnitten. Trots denna brist i vår undersökning tror vi att resultatet kan vara applicerbart även på övriga webbläsare.

Både observation och intervju är subjektiva metoder som kan ta lång tid att genomföra. Faran med subjektivitet är att risken för bias, så kallad skevhet, ökar (Bell, 2006 s. 158). För att undvika bias har vi lagt ner mycket tid på att formulera intervjufrågorna. Bias kan ha flera orsaker. Vi är trots allt “bara människor” och det är respondenternas högst subjektiva åsikter som ligger till grund för det insamlade dataunderlaget (Bell, 2006 s. 167). Vi har utgått från vår egen förförståelse och de resultat som tagits fram genom undersökningen är baserad på våra försökspersoners förförståelse när det kommer till att använda en webbläsare.

Gällande användarstudier ser vi att det kan finnas en generell risk i att man har gjort en bild av den ideala användaren och sedan speglar det på försökspersonen som testats. Detta var dock en risk som inte realiserades i vår undersökning då vi istället utgick från att försökspersonerna troligtvis skulle ha vissa svårigheter med respektive scenario. Avsikten med användarstudierna var till viss del att framkalla och observera fel och problem för försökspersonerna. Därför hade vi i förväg inte föreställt oss en ideal typ av användare då vårt syfte med undersökningen var att leta efter och observera svårigheter och problem för att identifiera dessa i gränssnittet.

Man får ha i åtanke att vi skapade scenarion för att observera specifika situationer och hade försökspersonerna ställts inför de svårigheterna i sin vardag hade utfallet av undersökningen kanske sett annorlunda ut. Försökspersonerna blev i princip "tvingade" till att slutföra uppgiften då vi inte gav dem utrymme för att ge upp. Det hade, ser vi i efterhand, varit en intressant aspekt att observera hur många som skulle valt att ge upp. Vi såg tendenser till att några ville avsluta uppgiften när det blev för svårt. Detta hade kunnat bekräfta Furnells tes att om säkerhet blir för svårt ger användaren upp (Furnell et al., 2005, s. 28).

10 Vidareforskning

Då denna undersökning enbart hade åtta försökspersoner som observerades i webbläsaren Chrome ser vi ett behov av att utföra mer omfattande studier. Några förslag är att undersöka fler användare och webbläsare samt fler uppgifter/scenarion för att få ett bredare underlag. Vi ser även en möjlighet att använda vår studie för framtida workshops, designförslag, användartester etcetera, som kan användas för att ta fram en webbläsare anpassad efter användarna och deras säkerhetsbehov.

Vi tror att framtidens webbläsare kan utvecklas på ett sätt som möjliggör att alla som surfar ska få möjlighet att upptäcka och åtgärda sina egna säkerhetsbehov på ett enkelt sätt. Utförs fler studier inom detta område tror vi att det finns en sannolikhet att vi i framtiden får en webbläsare som sprider kunskap och medvetenhet om säkerhet. En webbläsare på användarnas villkor, oavsett vilken typ av användare man är (från noviser till experter).

11 Litteraturförteckning

Bell, Judith (2006). *Introduktion till forskningsmetodik. 4.*, [uppdaterade] uppl. Lund: Studentlitteratur

Blomberg, J. (2003). *An Ethnographic Approach to Design*. J.A. Jacko and A. Sears, Eds. The human-computer interaction handbook: fundamentals, evolving technologies and emerging applications, pp. 964-986. New Jersey: Lawrence Erlbaum Associates, Inc.

Friedman, B., Hurley, D., C. Howe, D., Felten, Edward., Nissenbaum, Helen. (2002) *Users' Conceptions of Web Security: A Comparative Study*. CHI 2002, pp. 746-747.

Furnell, S. (2009). *The irreverseble march of technology*. Information Security Technical Report, vol. 14, no. 4, pp. 176-180.

Furnell, S., Jusoh, A. & Katsabas, D. (2005). *The challenges of understanding and using security: A survey of end-users.* Computers & Security, vol. 25, iss. 1, pp. 27-35, 2006.

Google. (2014). *Surfa privat (inkognitoläge).* <https://support.google.com/chrome/answer/95464> [2014-12-15]

Ipeer. (2012). *Vad innebär SSL och vad är ett SSL-certifikat?* [blogg], 27 mars <http://www.ipeerhosting.se/vad-innebar-ssl-och-vad-ar-ett-ssl-certifikat/> [2015-01-05]

Mina Cookies, *REKOMMENDATION – SE* <http://www.minacookies.se/rekommendation-se/#Cookies> [2014-09-29]

Niederst Robbins, Jennifer (2012). *Learning web design: a beginner's guide to HTML, CSS, JavaScript and web graphics*. 4th ed. Sebastopol, CA: O'Reilly

Serrhini, M. & Moussa, A.A. (2013). *Home users security and the web browser inbuilt settings, framework to setup it automatically.* J. Comput. Sci., 9: pp. 159-168.

Symantec. (u.å). *Introduktion till SSL*. <http://www.symantec.com/sv/se/theme.jsp?themeid=how-ssl-works> [2015-01-05]

Thurén, Torsten (2007). *Vetenskapsteori för nybörjare*. 2., [omarb.] uppl. Stockholm: Liber

W3Schools. (2014). *Browser Statistics*. <http://www.w3schools.com/browsers/browsers_stats.asp> [2014-12-15]

Wahlberg, T., Paakkola, P., Wieser, C., Laakso, M., & Röning, J. (2013). *Kepler - Raising Browser Security Awareness*. Software Testing, Verification and Validation Workshops (ICSTW), 2013 IEEE Sixth International Conference, pp. 435-440.

Whalen, T. & Inkpen, K. M. (2005). *Gathering Evidence: Use of Visual Security Cues in Web Browsers*. Proceedings of Graphics Interface 2005, pp. 137-144.

Wisniewski, C. (2012). Which browser is safest? The browser wars are back and this time you win. *Naked Security* [blogg], 16 juli. <https://nakedsecurity.sophos.com/2012/07/16/which-browser-is-safest-the-browser-wars-are-back-and-this-time-you-win/> [2014-12-15]

12 Appendix

12.1 Bilaga 1

Samtyckeskontrakt gällande observationsstudie

Detta kontrakt har upprättats mellan dig som försöksperson och oss studenter för att klargöra dina rättigheter samt våra skyldigheter i hanteringen av din personliga information.

- Användarstudien vi kommer att utföra går ut på att undersöka användbarheten för webbläsaren Chrome. Användarstudien är en observation uppdelad i tre scenarion med några frågor efter varje scenario. Det vi undersöker är hur du uppfattar design, information och hur det är att använda webbläsaren Chrome.

- Resultatet som vi får fram genom observationerna och efterföljande intervjufrågor kommer att användas som analysunderlag till vår C-uppsats som skrivs under höstterminen 2014.

- Du kommer i presentationen av resultatet i uppsatsen att förbli anonym. Detta innebär att ditt namn och dina personuppgifter inte kommer att lämnas ut till någon annan än de som aktivt arbetar med uppsatsen. I detta fall innebär det att två studenter (vi som utför observationen) samt de lärare som handleder och examinerar kommer kunna ta del av informationen. Den slutgiltiga uppsatsen som publiceras på DiVA* kommer **inte** att innehålla information som kopplas till dig som person.

- Det inspelade materialet kommer endast att användas som minnesunderlag för oss. När uppsatsen är publicerad kommer det inspelade materialet därför också att raderas.

Genom att skriva på detta kontrakt samtycker du till punkterna ovan.

_____
Signatur / datum

_____ _____
Signatur Ida Eriksson Signatur Johanna Lundgren

Södertörns högskola

*DiVA är en databas som innehåller uppsatser i fulltext, men även publikationer från högskolans forskare. Många lärosäten har en DiVA-databas. Det går att söka i alla på en gång, eller välja att bara söka bland Södertörns högskolas publikationer.

12.2 Bilaga 2

Hej!

Vi är två studenter från Södertörns högskola som just nu går sista året på programmet IT, medier och design. Just nu söker vi försökspersoner till vår C-uppsats. Kanske just du vill och kan hjälpa oss?

Vi undersöker användbarheten för webbläsaren Chrome. Vår användarstudie är en observation uppdelad i tre scenarion med några frågor efter varje scenario. Det vi undersöker är hur du uppfattar design, information och hur det är att använda webbläsaren Chrome.

Tidsåtgången för varje test beräknas till cirka en timme per användare.

Det som krävs för att kunna ställa upp är att:

- du har en egen dator
- du har webbläsaren Chrome installerad på din dator
- det finns uppkoppling hemma hos dig/där du vill möta upp oss

Vi kommer gemensamt överens om tid och plats för observationen, dock behöver vi vara på en ostörd plats. Observationerna kommer att ske mellan den 5/12-17/12 2014.

Självklart tar vi med fika!

Låter detta intressant och som något för dig?

Hör av dig till:
Ida Eriksson (namn@mail.com) eller Johanna Lundgren (namn@mail.com).

Vänligen
Ida och Johanna

12.3 Bilaga 3

Observationsscheman

x = rätt klick, - = felklick

Scenario 1																				
Klick:																				
Hur löstes uppgiften? Webbläsare = W, Google = G																				

Scenario 2																				
Klick:																				

12.4 Bilaga 4

Intervjufrågor
Vad betyder “surfa säkert” för dig?
Hur surfar du säkert idag?

Scenario 1

- Visste du vad funktionen var för någonting sedan innan?
    - Om ja, har du använt funktionen tidigare? Vid vilka typer av tillfällen?
    - Om nej, hade du velat att webbläsaren presenterar den här funktionen?

- Vet du vad funktionen gör?

- Tycker du att namnet på funktionen motsvarar det den faktiskt gör? (Dvs att den tar bort webbhistorik, cookies, lösenord etcetera när webbläsarfönstret stängs ner.)

- Ser du skillnad på när du surfar inkognito mot när du surfar vanligt i webbläsaren?

- Upplever du funktionen som relevant? Ser du varför skulle man behöva den?
    - I vilka sammanhang tror du det kan vara relevant att använda funktionen?
    - Från vem kan det vara bra att skydda information ifrån?

- Tycker du funktionen är lätt att använda?

- Har du några förslag på hur man skulle kunna förbättra den här funktionen?

Scenario 2

- Förstår du vad ikonen innebär?

- Visste du vad du skulle leta efter i inställningarna för att komma på rätt väg när du löste uppgiften?

- Upplever du de olika stegen för att ändra inställningen som logiska?
    - Tycker du att terminologin är förståelig under inställningar?
        - Förstår du vad *visa avancerade inställningar* betyder i det här sammanhanget?
        - Vad betyder ordet sekretess för dig?
        - Förstår du vad rubriken innehållsinställningar betyder?
        - Tycker du att blockering av tredjepartscookies ligger på rätt plats?
    - Kände du att du var på rätt väg efter varje steg?

- Tycker du att det är lätt att hitta vart du ändrar inställningarna?

- Känner du dig säker med att navigera dig runt i menyn?

- Vet du vem tredjepart är?

- Har du blockerat tredjepartcookies tidigare?

- Tycker du att gränssnittet i webbläsaren berättar om konsekvenserna med olika funktioner?

- Har du några förslag på hur man skulle kunna förbättra utseendet och rubrikerna i inställningspanelen?

Scenario 3
Börja med att jämföra ikonerna på varje flik

- Har du sett den här ikonen tidigare?
    - Vad symboliserar ikonen för dig?

- Har du klickat på någon av de här ikonerna tidigare?
    - Varför/varför inte?

Be användaren att läsa under varje ikon på varje sida

- Förstår du informationen du får när du klickar på ikonen?

- Informationen du fick, var det vad du förväntade dig när du klickade på ikonen?

- Känns informationen viktig/relevant för dig som användare?

- Hur tolkar du informationen du får från de olika sidorna?
    - Tycker du att informationen framgår på ett tydligt sätt?
    - Hur får informationen dig att känna angående din säkerhet?

- Hur upplevde du informationen?
    - Hur upplevde du terminologin?
    - Ville du lära dig mer efter att ha läst om de olika anslutningarna?

- Har du några förslag på hur man skulle kunna förbättra den här funktionen?
    - Hur skulle du vilja att ikonerna presenteras?