Kandidatuppsats

Digital Design & Innovation 180 hp

Är du medveten om säkerhetsrisker i ditt smarta hem?

En designstudie över hur digitala knuffar kan designas för att stödja medvetenhet kring IoT-säkerhetsrisker i det smarta hemmet

Informatik 15 hp

Halmstad 3/6-22
Arvid Gulin & James Holmgren

HÖGSKOLAN
I HALMSTAD

Abstrakt

I hänsyn till att Internet of Things (IoT) fortsätter implementeras i privata hem blir säkerhets- och integritetsfrågor allt viktigare. Tidigare studier har visat att det finns flera olika säkerhetsrisker med IoT och smarta hem. Dessa är däremot ofta mycket tekniska och inte lätta att förstå för användare vilket lämnar användare omedvetna om potentiella säkerhetsrisker. Studien har undersökt användares medvetenhet om de säkerhetsrisker som ingår vid användning av IoT i smarta hem. Under studien har en narrativ litteraturstudie genomförts för att utforska tidigare forskning. En prototyp bestående av fyra olika designelement har skapats baserat på heuristiker och designprinciper. Prototypen har därefter använt för att undersöka hur digitala knuffar kan designas för att stödja användares medvetenhet kring IoT-säkerhetsrisker i smarta hem. Utvärderingstester genomfördes med totalt tio användare för att studera hur digitala knuffar kan designas för att stödja användarnas medvetenhet om potentiella säkerhetsrisker i smarta hem. Studien resulterar i fyra designförslag för hur digitala knuffar kan designas för att stödja användarnas medvetenhet kring IoT-säkerhetsrisker i det smarta hemmet.

Nyckelord: *Internet of Things, Säkerhetsrisker, Smarta hem, Medvetenhet, Digitala knuffar.*

Abstract

With the increasing use of Internet of Things (IoT) in private homes the security and privacy issues become increasingly important. Previous studies have highlighted that there are several different security risks with IoT and smart homes. However, these are often very technical and not easily understood for users which leaves the users unaware of potential security risks. This study has investigated users' awareness about the security risks that are included when using IoT in the smart home environment. During the study a narrative literature study has been conducted to explore previous research. A prototype consisting of four different design elements has been created based on heuristics and design principles. The prototype has then been used to study how digital nudges can be designed to support users' awareness in regard to IoT security risks in smart homes. Evaluation tests were performed with a total of ten users to study how digital nudges can be designed to support users' awareness of potential security risks in smart homes. The study results in four design proposals for how digital nudges can be designed to support users' awareness of IoT-security issues in the smart home environment.

Keywords: *Internet of Things, Security risks, Smart home, Awareness, Digital nudges.*

Förord

Vi vill i första hand tacka vår handledare Oliver Weberg för de värdefulla råd, diskussioner och feedback vi fått under arbetet. Samtidigt vill vi tacka alla som har deltagit i studien vilket varit avgörande för dess genomförande och resultat. Avslutningsvis vill vi tacka de opponenter och övriga handledare som bidragit med konstruktiv kritik under studien.

Arvid Gulin

James Holmgren

Innehållsförteckning

1 Introduktion

Internet of Things (IoT) består av enheter som är uppkopplade till internet, vilket samlar och delar information mellan varandra (Bandyopadhyay & Sen, 2011; Koohang et al., 2022; Yang et al., 2017). I samband med utvecklingen av IoT har det implementerats i flera användningsområden bland annat i privata hushåll (Almusaylim & Zaman, 2019; Koohang et al., 2022). Utvecklingen av IoT har möjliggjort för traditionella hem att bli "smarta". Det smarta hemmet är ett hushåll som med hjälp av sensorer, system och enheter kan nås på distans, kontrolleras och övervakas (Almusaylim & Zaman, 2019). Det smarta hemmet underlättar uppgifter i vardagen, några exempel är belysning som kan justeras via telefonen, automatiserad städning eller säkerhetslarm som kan skicka notiser till användaren (Ando et al., 2016).

IoT är under ständig tillväxt och år 2025 förväntas det finnas 75.44 miljarder uppkopplade enheter (Zhou et al., 2018). I takt med att det tillkommer fler IoT-enheter och de blir allt vanligare i privata hem blir säkerhetsriskerna och medvetenheten om dessa allt mer aktuella att utforska. Bakgrunden till att säkerhetsbristerna existerar är för att IoT-tillverkarna prioriterar funktionalitet framför säkerhetshetsåtgärder (Koohang et al., 2022; Neshenko et al., 2019). En annan anledning är att IoT-enheter har begränsad hårdvara vilket gör det svårt att implementera nödvändiga säkerhetsfunktioner (Neshenko et al., 2019). Resultatet av säkerhetsriskerna blir att ansvaret hamnar på användarna, däremot anser användare generellt att det är tillverkarna som ska hållas ansvariga (Koohang et al., 2022; Neshenko et al., 2019). De medföljande säkerhetsriskerna innefattar att obehöriga kan få tillgång till enheter och åtkomst till personlig data, nätverk och även andra uppkopplade enheter (Sivaraman et al., 2015). Dessa säkerhetsrisker har användare bristande medvetenhet om (Koohang et al., 2022). I en studie utförd av Neshenko et al. (2019) framkommer det att 48% av användare inte är medvetna om säkerhetsrisker i det smarta hemmet. Medvetenhet angående säkerhetsrisker inom IoT hos användare är bristfällig (Koohang et al., 2022; Rice & Bogdanov, 2019; Neshenko et al., 2019) och det saknas ett funktionellt sätt för att bemöta detta (Rice & Bogdanov, 2019; Streiff et al., 2019). Brist på medvetenhet om de risker som finns begränsar således valalternativ och leder till att användare har svårt att förstå och bemöta säkerhetsrisker (Kraemer et al., 2009; Neshenko et al., 2019). Att användares medvetenhet kring säkerhetsrisker är bristande har framställts att det delvis beror på bristfälliga säkerhetsåtgärder (Koohang et al., 2022; Neshenko et al., 2019). De säkerhetsrisker som användare riskerar att utsättas för kan resultera i att obehöriga får tillgång till användarens privata data och exponeras för eventuella cyberattacker (De Bruijn & Janssen, 2017; Kang & Kim, 2017; Neshenko et al., 2019).

Det har identifierats att knuffar, även kallade nudges, är olika sätt att influera människors omdöme, val och beteende (Acquisti et al., 2017; Hansen, 2016; Thaler & Sunstein, 2008). Knuffar har ökat i användning i digitala användningsområden i samband med utvecklingen av digitala gränssnitt (Mirsch et al., 2017; Schneider et al., 2018). Knuffar i digitala miljöer, digitala knuffar, kan vara ett effektivt verktyg för att vägleda användares beslutsfattande och påverka beteende (Mirsch et al., 2017). Det finns etiska diskussioner om hur digitala knuffar ska designas, det är bland annat viktigt att knuffar som designas inte förhindrar eller begränsar valalternativ (Hansen, 2016; Mirsch et al., 2017; Thaler & Sunstein, 2008). Då knuffar kan användas för att påverka individers beteende är det även viktigt att de implementeras med god avsikt och tillåter för personer att ta gynnsamma beslut (Hansen, 2016; Mirsch et al., 2017; Thaler & Sunstein, 2008).

Tidigare forskning kring digitala knuffar har primärt använts för att studera hur knuffar kan influera människor mot en mer hälsosam livsstil eller hållbart beteende (Mirsch et al., 2017; Schneider et al., 2018; Weinmann et al., 2016). Det har framställts designprinciper för hur digitala knuffar kan designas (Thaler et al., 2010; Weinmann et al., 2016). Dessa designprinciper är övergripande riktlinjer och inte inriktade för en specifik kontext samtidigt som de inte har använts för att studera hur medvetenhet kan stödjas. I samband med att användare har bristande medvetenhet om IoT-säkerhetsrisker och att knuffar inte tidigare använts för att studera hur de kan stödja medvetenhet har det blivit studiens infallsvinkel. För att undersöka detta har studien avsett att besvara frågeställningen:

Hur kan digitala knuffar designas för att stödja användares medvetenhet kring IoT-säkerhetsrisker i smarta hem?

2 Relaterad litteratur

Detta avsnitt presenterar resultatet av litteraturstudien och redogör för begrepp, teorier och tidigare forskning inom området som är relevanta för att besvara studiens frågeställning. Avsnittet inleds med beskrivning över IoT, smarta hem, vilka säkerhetsrisker som medföljer samt användares medvetenheten kring dessa. Ytterligare förklaras faserna för medvetenhet, knuffar, digitala knuffar, heuristiker samt designprinciper för digitala knuffar. Avsnittet avslutas med en sammanfattning över samtlig relaterad litteratur.

2.1 Internet of Things

IoT är ett gemensamt namn för enheter som samlar och delar data mellan varandra genom sensorer, mjukvara och anslutning till internet (Bandyopadhyay & Sen, 2011; Koohang et al., 2022; Yang et al., 2017). Dessa enheter har ett stort antal användningsområden och implementeras idag i bland annat privatpersoners hushåll, industriella miljöer, städer och fordon (Yang et al., 2017). Under de senaste åren har antalet uppkopplade IoT-enheter ökat och vid år 2025 förväntas det finnas omkring 75.44 miljarder enheter uppkopplade (Zhou et al., 2018). I Barcelona har IoT använts för att digitalisera och göra staden smartare (Lakhwani et al., 2020). Staden implementerade sensorer i gatubelysning som möjliggjorde för att anpassa ljusstyrka beroende på om det var personer närvarande eller inte. Resultatet bidrog till miljösmart gatubelysning och mindre ekonomisk belastning för staden (Lakhwani et al., 2020). Ur ett industriellt perspektiv finns det fördelar med att tillämpa IoT inom exempelvis industriell tillverkning, automation, transport och logistik (Bandyopadhyay & Sen, 2011). Ur en privat användares synvinkel kommer de mest uppenbara effekterna av IoT att vara både i hemmet och på arbetsplatsen. Smarta hem, kontor och hemtjänst är exempel på möjliga tillämpningsområden där IoT kan göra skillnad (Bandyopadhyay & Sen, 2011).

2.1.1 Smarta hem

Ett smart hem är ett hem som har olika IoT-enheter uppkopplade och möjliggör att utföra åtgärder utan användarinput och kan hanteras genom en central kontrollenhet, exempelvis en smartphone (Al-Mutawa & Eassa, 2020; Almusaylim & Zaman, 2019). Smarta hem kan användas för att förenkla användarens vardagliga liv vilket kan göras på två sätt. Ett sätt är att smarta hem lär sig användarens beteendemönster och därefter automatiserar uppgifter för att optimera bekvämligheten (Alam et al., 2012). Exempelvis kan det minska energianvändningen i ett hushåll genom att analysera användarbeteendet (Alam et al., 2012). Det andra sättet är att

smarta hem kan förenkla användares vardagliga liv genom möjliggöra att det kan kontrolleras och bevakas på distans (Alam et al., 2012).

Smarta hem kan även bidra med sjukvårdstjänster till dess användare. Vid 2050 beräknas det att sjukhus och vårdcentraler inte kommer ha plats för att assistera alla patienter med kroniska sjukdomar (Alam et al., 2012). Den framtida lösningen på problemet kan bli smarta hem som skulle kunna avlasta sjukvården (Alam et al., 2012). Detta skulle utföras genom att smarta hem samlar information från patienter och informerar läkare om deras hälsotillstånd, försäkrar personlig assistans vid behov samt vid nödsituationer tillkallar sjukvård (Alam et al., 2012).

2.2 Säkerhetsrisker inom IoT och smarta hem

Tillverkare av IoT-enheter prioriterar ökad funktionalitet framför säkerhet vilket leder till att ansvaret hamnar på slutanvändaren (Koohang et al., 2022). På grund av vinstdrivna företag samt brist på lagar och regleringar inom området möjliggör för tillverkare att förbise säkerhetsåtgärder och designa potentiellt sårbara IoT-enheter (Neshenko et al., 2019). Ytterligare en anledning varför det är svårt att applicera tillräckliga säkerhetsfunktioner i IoT-enheter är på grund av att enheterna ofta har fysiska begränsningar som bland annat data- och batterikapacitet (Yang et al., 2017). Detta gör att enheterna inte har möjlighet att implementera de säkerhetsåtgärder som krävs vilket möjliggör för obehöriga att få tillgång till enheterna utan större ansträngning (Neshenko et al., 2019).

De flesta cyberattacker är ofarliga men det förekommer skadliga dataintrång som kan leda till att obehöriga får tillgång till och kan manipulera personlig data, utföra ID-stölder eller få åtkomst till hela system (De Bruijn & Janssen, 2017). Exempelvis om en användare har utfört köp via en uppkopplad Smart TV och den blir hackad kan användarens betalningsinformation läckas (Kang & Kim, 2017). Almusaylim & Zaman (2019) menar även på att risken att utsättas för cyberattacker ökar med mängden uppkopplade enheter som finns tillgängliga i hemmet. I samband med att enheter ansluts till nätverket utsätts användarna för säkerhetsrisker då personlig data riskerar att exponeras för cyberattacker (Almusaylim & Zaman, 2019).

Hemmet som tidigare var en privat plats blir mer exponerat till följd av digitaliseringens utveckling och medföljande säkerhetsrisker lämnar användarens integritet exponerad (Almusaylim & Zaman, 2019). Smarta hem kan därmed hota användarens rätt att kontrollera sin personliga data och informationsintegritet (Lee, 2020). De säkerhetsrisker som finns hos IoT-enheter tydliggörs sällan för konsumenter (Streiff et al., 2019). Även de säkerhetsåtgärder som faktiskt finns i IoT-enheter i smarta hem är

bristfälliga och användare behöver bli mer medvetna om de säkerhetsbrister och risker som finns för att kunna skydda sig (Almusaylim & Zaman, 2019).

2.3 Användares medvetenhet om säkerhetsrisker

Vissa tillverkare implementerar säkerhetsåtgärder i sina IoT-enheter som exempelvis mjukvaruuppdateringar men dessa kan vara för tekniskt komplicerade för användare att installera (Neshenko et al., 2019). I en studie om IoT-enheters säkerhet uttrycker 40% av användare att de aldrig utfört mjukvaruuppdateringar för att öka säkerheten för sin enhet (Neshenko et al., 2019). Komplicerade säkerhetssystem, svårtolkade säkerhetsvillkor och bristande kunskap leder till att användare har svårt att hantera samt förstå säkerhetsrisker (Kraemer et al., 2009).

Det framkommer även att användare anser att det är tillverkaren som bär ansvaret för IoT-enhetens säkerhet, vilket resulterar i att användare inte utbildar sig i hur de kan öka säkerheten (Neshenko et al., 2019). Användare anser generellt att säkerhet och integritet är viktiga aspekter, däremot finns det brist på kunskap avseende de säkerhetsrisker som IoT-enheter i hemmet medför (Koohang et al., 2022). Detta bekräftas i en studie som framhäver att användare generellt är dåligt informerade om hur deras data insamlas och används (Rice & Bogdanov, 2019). I samband med utvecklingen av IoT har det även blivit lättare att installera IoT-enheter i hemmet utan större teknisk erfarenhet (Gilchrist, 2017). En stor del av användare har inget behov av att lära sig det tekniska utan vill bara använda IoT och dra nytta av de positiva aspekterna, trots säkerhetsriskerna (Gilchrist, 2017; Wang et al., 2018).

Det fastställs i en studie gällande internetsäkerhet att uppemot 48% av användare inte har kunskap om de säkerhetsrisker som finns inom IoT (Neshenko et al., 2019). Det är även fastställt att de användare som har medvetenhet gällande riskerna inte har tillräckligt med kunskap om vad de behöver göra för att undvika dessa (Neshenko et al., 2019). I en artikel utforskades användares medvetenhet krings säkerhet- och integritetsrisker relaterat till smart TV varav resultatet framhävde att endast 16% uppvisar en medvetenhet om de relaterade riskerna (Legg, 2016). Studien förklarar även att det är mer sannolikt att användare implementerar säkerhetsåtgärder om det inte påverkar enhetens funktionalitet (Legg, 2016).

Det är viktigt att tillverkarna framhäver vilka specifikationer IoT-enheterna har, vad säkerhetsriskerna med dessa kan vara, samt vad användaren själv kan göra för att öka säkerheten (Streiff et al., 2019). Det argumenteras för att det saknas ett funktionellt sätt att informera användare om hur deras data hanteras (Rice & Bogdanov, 2019). Samtidigt finns ett behov att undersöka olika tillvägagångssätt för att öka användares medvetenhet kring säkerhetsrisker vid IoT för att minska sannolikheten att deras data exponeras (Neshenko et al., 2019). I Japan, när en tjänsteleverantör klarar en

tredjeparts inspektion, angående integritet och säkerhet, blir de tilldelade en förtroendestämpel (Ando et al., 2016). Syftet med stämpeln är att minska användare oro kring webbplatsanvändning samt gör de mer upplysta om eventuella risker (Ando et al., 2016). Däremot i samband med IoT-enheter hastigt ökade spridning är det essentiellt att nya metoder skapas för att förhindra säkerhet- och integritetsrisker (Ando et al., 2016).

Forskning framhäver att det finns bristande medvetenhet hos användare angående säkerhetsrisker på nätet och internetrelaterade applikationer (Zwilling et al., 2022). En studie poängterar på hur respondenter med låg medvetenhet dock har en aning om att det finns risker med att vara uppkopplad online (Zwilling et al., 2022). Studien betonar även på att användare med låg medvetenhet om risker inte utför åtgärder för att förebygga att problemen medan användare med en högre medvetenhet om hot och risker skyddar sig.

En studie som undersökt om användare kan identifiera om en IoT-enhet har blivit utsatt för cyberattack eller fått virus bevisar att användare har svårt att identifiera hoten (McDermot et al., 2019). Anledningen är för att det inte framkommer tydliga indikatorer att enheten har blivit utsatt för intrång (McDermot et al., 2019). Resultatet visar på att det inte är den tekniska erfarenheten hos användare som är problemet utan det är brist på information som IoT-enheterna presenterar (McDermot et al., 2019).

2.4 Medvetenhet

För att människor ska agera med omvärlden behöver de en uppfattning om vad som händer, denna förståelse förklaras som medvetenhet, personers kunskap om en miljös tillstånd (Niemantsverdriet et al., 2019). Då tillstånd i olika miljöer kan förändras finns det ett behov av att medvetenhet underhålls. Det är på grund av medvetenhet om sin omgivning som människor kan förstå en situation, förutse, sätta upp mål, agera och utvärdera resultat (Niemantsverdriet et al., 2019).

I en studie om företags datahantering från konsumenter har medvetenhet använts till vilken grad konsumenter har förståelse för hur verksamheter insamlar och nyttjar data (Rice & Bogdanov, 2019). I IoT-kontext definieras medvetenhet som den nivå vilket användare har kunskap kring de uppstående och ökade säkerhetshoten som uppstår med IoT och hur frekvent de uppstår (Koohang et al., 2022).

Medvetenhet har inte en tydlig gemensam definition, däremot är det viktigt att uppmärksamma att begreppet handlar om en användares interna kunskap och förståelse av en situation (Gross, 2013). Detta inkluderar andra människor och omgivningen vilket tolkas genom subtila metoder för att fånga och tolka information (Gross, 2013). Gemensamt för flera studier är att medvetenhet innefattar produkt, kunskap som en person kan använda,

och process, hur den kunskapen skapas genom interaktion med miljö (Gutwin & Greenberg, 2002; Gross, 2013).

I en definition avseende situationsmedvetenhet, medvetenhet i en viss situation, beskrivs det hur en person kontinuerligt samlar information från sin miljö och integrerar den med tidigare kunskap och sammanställer det för att använda till framtida händelser (Endsley, 1995). Det kan även definieras som kombinationen av redan existerande och ny kunskap vilket bidrar till utvecklingen av sammanfattad förståelse av den nuvarande situationen och framtida situationer och även medföljande konsekvenser som förekommer (Endsley, 1995). Ur processen för hur personer skapar kunskap genom interaktion med miljö har Endsley (1995) fastställt tre faser. Dessa är uppfattning, förståelse och slutligen agera. För att uppnå medvetenhet är samtliga faser nödvändiga men en delvis medvetenhet kan uppnås trots att alla faser inte bemöts (Endsley, 1995).

2.4.1 Uppfattning

Den första fasen för att uppnå medvetenhet är att uppfatta status, attribut och olika samband i relevanta element i ens miljö (Endsley, 2001). En person måste kunna samla in information från sin omgivning för att sedan välja vilken information som är relevant och inte (Endsley, 1995). Uppfattning kan begränsas beroende på individens mål, förväntningar eller tidigare erfarenheter (Endsley & Garland, 2000). Under detta stadie är det viktigt att vara observant och sortera vilken information som är viktig för att sedan skapa sig en förståelse i senare stadie (Endsley & Garland, 2000).

2.4.2 Förståelse

Den andra fasen för att uppnå medvetenhet är att skapa en förståelse av de olika element som insamlats under uppfattning (Endsley, 2001). En person behöver skapa sig en förståelse för informationen och med befintlig kunskap reflektera och agera (Endsley, 1995). För att få en förståelse behöver personer samla, kombinera och tolka information (Endsley & Garland 2000). Det innebär alltså att information som uppfattas behöver bearbetas av personer för att förstå den och tolka hur den är relevant för deras mål (Endsley, 1995).

2.4.3 Agera

Sista fasen för att uppnå medvetenhet är att projicera framtida händelser genom kunskap om olika element och en förståelse för situationen (Endsley, 2001). För en person att kunna använda informationen behöver den ha en uppfattning om konsekvenser och förutse inverkan av olika beslut (Endsley, 1995). Förståelse för konsekvenser och att förutse eventuella effekter med information möjliggör för personer att agera (Endsley & Garland, 2000).

2.5 Knuffar

Knuffar, även kallade nudges, är funktioner som försöker påverka människors omdöme, val eller beteende på ett förutsägbart vis utan att förhindra andra val (Hansen, 2016; Thaler & Sunstein, 2008). Det förutsägbara viset som personer påverkas av knuffar möjliggörs av kognitiva funktioner, fördomar, rutiner och vanor (Hansen, 2016). Knuffar ska användas för att tillåta människor att ta bättre beslut men aldrig ske på bekostnad av personens fria vilja (Hansen, 2016; Mirsch et al., 2017; Thaler & Sunstein, 2008). Acquisti (2009) uttrycker att knuffar kan implementeras för att exempelvis stödja säkerhet och integritet i digitala sammanhang.

Då knuffar kan användas för att påverka individers beteende är det viktigt att knuffarna implementeras med god avsikt för att göra det lättare för personer att göra bättre val (Acquisti et al., 2017; Hansen, 2016; Thaler & Sunstein, 2008). Det finns etiska diskussioner om hur knuffar ska designas för att god avsikt kan variera från person (Thaler & Sunstein, 2008). Det är därför viktigt att knuffar designas utan att förhindra eller begränsa valalternativen (Hansen, 2016; Mirsch et al., 2017; Thaler & Sunstein, 2008).

2.6 Digitala knuffar

Knuffar har ökat i användning i digitala användningsområden då fler val och beslut tas via ett digitalt gränssnitt (Mirsch et al., 2017; Schneider et al., 2018). Digitala knuffar definieras som användningen av designelement i gränssnitt för att vägleda eller påverka personers val i en digital miljö (Weinmann et al., 2016). Människor tenderar att ta ogynnsamma beslut på grund av att de utsätts för stor mängd information i digitala miljöer, dessa digitala miljöer kan vara dator- eller mobilskärmar exempelvis (Mirsch et al., 2017). Knuffar kan vara ett effektivt verktyg att använda i den digitala miljön för att vägleda användares beslutsfattande (Mirsch et al., 2017).

Digitala knuffar lägger ofta fokus på människors val men konceptet kan tillämpas i andra sammanhang för andra syften (Weinmann et al., 2016). Digitala knuffar har använts i andra studier bland annat för att uppmuntra användare att koppla sina mobiltelefoner till mer säkra wifi-nätverk genom färgkodning (Turland et al., 2015). I en studie inom e-handel testades sju olika former av digitala knuffar för att se hur de kan påverka konsumenters köpvanor som visar på att konsumenter kan påverkas olika vis beroende på vilka knuffar som används (Dennis et al., 2020). I en annan studie identifierades att ställa frågor vid rätt tillfälle till Facebookanvändare avseende vad för innehåll de delar var det tillräckligt för att ändra deras användarbeteende (Gross & Acquisti, 2005).

Att implementera knuffar i ett digitalt sammanhang kan vara kostnadseffektivt, enkelt och snabbt (Weinmann et al., 2016). Dessutom möjliggör internet för funktioner som användare spårning som kan underlätta personalisering av knuffar vilket potentiellt kan göra de mer effektiva (Weinmann et al., 2016). Knuffar i den digitala miljön kan formas efter användarens personliga preferenser för att på så vis vara mer användbara (Schneider et al., 2018).

2.6.1 Designprinciper för digitala knuffar

Designprinciper för digitala knuffar är användbara för att vägleda människor mot bättre val (Thaler et al., 2010; Weinmann et al., 2016). Designprinciperna som Thaler et al. (2010) framställt och Weinmann et al. (2016) vidareutvecklat kan användas för att vägleda utan att förhindra personers valmöjligheter vid digitala knuffar. Det finns totalt sex stycken designprinciper: incitament, kartläggning, standard, feedback, förväntade fel och strukturkomplexa val. Samtliga redovisas i nedanstående rubriker.

Incitament

Incitament syftar till att skapa lämplig motivation för personer och att därmed knuffa åt bättre val (Weinmann et al., 2016). För att möjliggöra detta bör incitament framträda tydligt för vara mest effektiv (Weinmann et al., 2016). Dessa incitament, eller motivationer, kan användas för att visa på vinster eller förluster med olika val (Weinmann et al., 2016). Exempelvis har personer olika motivationer och kan därför bemötas olika för att uppfylla individuella incitament (Thaler et al., 2010).

Kartläggning

Kartläggning behandlar att koppla svårtolkad information till något som är mer bekant för användaren (Weinmann et al., 2016). Att möjliggöra för användare att tolka information baserat på tidigare erfarenheter tillåter att förstå, tolka och välja olika alternativ (Weinmann et al., 2016). Exempelvis kan konsekvenser av olika alternativ presenteras för användare för att möjligöra beslutstagande (Thaler et al., 2010).

Standard

Standard handlar om att presentera förvalda alternativ då personer har en tendens att inte ändra val som är förinställda (Weinmann et al., 2016). Att implementera ett alternativ som är förvalt kan vara användbart för att få personer att ta bättre beslut (Weinmann et al., 2016). Exempelvis kan inställningar användas vid installation av ny programvara för att underlätta

att slutföra installation med de mest gynnsamma inställningarna (Thaler et al., 2010).

Feedback

Feedback ger användare respons när de tar olika val för att visa på om de tar bra eller dåliga alternativ (Weinmann et al., 2016). Principen bygger på att ge feedback till användare för att uppmärksamma om olika handlingar. Exempelvis kan en digitalkamera presentera användaren med en förhandsvisning av tagen bild för att visa att bilden blev tagen, att den blev bra och att det inte uppstod några problem (Thaler et al., 2010).

Förväntade fel

Förväntade fel är en princip som bygger på att förvänta sig att användare kan och kommer göra misstag samt ha överseende för detta (Weinmann et al., 2016). Exempelvis kan en tunnelbana biljett inläsas i maskinen oavsett vilket håll den stoppas in, detta för att möjliggöra för fel men även förebygga (Thaler et al., 2010).

Strukturkomplexa val

Strukturkomplexa val innebär att presentera samtliga alternativ för användare för att möjliggöra att göra avvägningar när det är nödvändigt (Weinmann et al., 2016). Det möjliggör för att förstå komplicerad information och jämföra olika val (Thaler et al., 2010). Exempelvis kan en samling över olika målarfärger i ett färghjul underlätta val istället för att endast se namn över olika färger (Thaler et al., 2010).

2.7 Heurustiker och fördomar vid beslutstagande

Människor är upptagna och kan inte att spendera all tid till att analysera varje beslutstagande, istället använder människor heuristiker för att tänka och agera (Thaler & Sunstein, 2008). Heuristiker kan nyttjas för att underlätta beslutsfattande genom att minska mängden information som behövs för att ta beslut (Schneider, 2018). Att förstå heuristiker och fördomar kan hjälpa designerns att guida människor vid beslutstagande (Schneider et al., 2018). De fyra heuristiker som är mest förekommande bland digitala knuffar är framing, status quo bias, social norms samt loss aversion (Mirsch et al., 2017).

2.7.1 Framing

Framing berör hur information presenteras för en människa (Thaler & Sunstein, 2008). Framing innebär att förmedla information på ett sätt som påverkar personer genom erfarenhet, värderingar och attityder (Chong & Druckman, 2007; Mirsch et al., 2017; Lehner et al., 2016). Det kan användas för att presentera information positivt eller negativt och det är därför viktigt vid design att presentera information olika beroende på syfte (Thaler & Sunstein, 2008). Information kan presenteras för att lyfta fram fördelarna med alternativen så att det uppfattas som en vinst istället för en förlust (Mirsch et al., 2017; Thaler & Sunstein, 2008). Exempelvis om en läkare presenterar hur många som överlever en operation kan patienten bli mer positiv till att genomföra den. Däremot om läkaren presenterar hur många som dör av en operation blir patienten mer kritisk till att genomföra den (Thaler & Sunstein, 2008).

2.7.2 Status Quo Bias

Status quo bias innebär att personer har ett stort behov av att förbli i samma situation då nackdelarna med att förändra situationen anses större än fördelarna (Mirsch et al., 2017). Det kan vara användbart att använda status quo bias vid förvalda alternativ (Mirsch et al., 2017). Status quo bias kan bero på att människor inte är uppmärksamma och väljer förvalda alternativ, oavsett om det inte är det mest fördelaktiga alternativet (Thaler & Sunstein, 2008). Människor upplever att det finns en anledning till att alternativ är förvalda och att det därmed är det bästa valet (Thaler & Sunstein, 2008). Status quo bias kan vara användbar när det finns flera alternativ och underlättar för beslutstagande (Thaler & Sunstein, 2008).

Förinställda alternativ kan assistera personer att ta beslut men det är viktigt att de designas rätt (Thaler & Sunstein, 2008). Det bör inte finnas för mycket information och status quo bias ska designas för att göra val enklare för personer (Thaler & Sunstein, 2008). För att designa status quo bias kan valalternativen spela roll (Thaler & Sunstein, 2008). Vid enklare val, där ja och nej, alternativ kan användas bör de användas (Thaler & Sunstein, 2008). Om valalternativen är svårare bör det finnas ett standardalternativ som är förinställt (Thaler & Sunstein, 2008). Exempelvis ger ett förinställt alternativ att vara organdonator betydligt fler organdonationer än om det inte var förinställt (Acquisti et al., 2017).

2.7.3 Loss aversion

Loss aversion innebär att personer har en stark vilja för att inte förlora, de undviker hellre förlust än erhåller en vinst (Thaler & Sunstein, 2008; Acquisti et al., 2017). För att designa för loss aversion kan begränsade- eller specialerbjudanden användas för att knuffa mot ett val (Mirsch et al., 2017).

Loss aversion baseras på hur personen värdesätter det de har och inte vill förlora det (Thaler & Sunstein, 2008). Loss aversion kan användas för att underlätta beslutsprocessen genom visuella element eller information för att visa på effekterna av att ta ett val (Mirsch et al., 2017). När personer äger något värdesätts det mer, men när känslan av att det är förlorat inträffar värdesätts det mindre (Acquisti et al., 2017).

I ett experiment utfört av Thaler & Sunstein (2008), för att visa på loss aversion fick hälften av eleverna i ett klassrum kaffemuggar och hälften fick en chokladkaka. Muggen och chokladen kostade ungefär lika mycket, och i ett förtest var eleverna lika benägna att välja den ena som den andra. Men när de erbjuds möjligheten att byta en kaffemugg mot en chokladkaka eller vice versa var det bara en av tio som bytte. Resultatet visar på att loss aversion knuffar mot att inte göra förändringar, även när det kan vara ett fördelaktigt alternativ (Thaler & Sunstein, 2008).

2.7.4 Social norms

Personer har lätt för att följa andra personers beteenden och val (Mirsch et al., 2017). Social norms grundar sig i sociala influenser vilket kan göra den sociala normen förutsägbar (Thaler & Sunstein, 2008). För att designa för social norms kan alltså information om hur andra personer agerat implementeras för att underlätta val (Thaler & Sunstein, 2008). Detta kan göras i form av statistik, text eller information som pekar på hur andra agerat (Hansen, 2016). Knuffen resulterar i att personer inte vill bryta den sociala normen (Thaler & Sunstein, 2008). Social norms har i en tidigare studie använts för att minska elkonsumtion. Genom att informera närliggandes hushålls elförbrukning influerades människor som förbrukar mer el att minska sin elkonsumtion (Thaler & Sunstein, 2008).

2.8 Sammanfattning av litteraturstudie

Tidigare forskning framhäver att det smarta hemmet genom hjälp av IoT-enheter gör användares vardag enklare men medför säkerhetsrisker (Almusaylim & Zaman, 2019; Ando et al., 2016; Koohang et al., 2022; Sivaraman et al., 2015; Yang et al., 2017). Dessa säkerhetsrisker kan medföra ID-stölder, dataintrång och manipulation av IoT-enheterna i hemmet (Almusaylim & Zaman, 2019; De Bruijn & Janssen, 2017).

Det har presenterats olika förklaringar avseende hur säkerhetsriskerna har uppstått. Yang et al. (2017) uttrycker att det beror på limitationerna i IoT-enheterna, framförallt begränsad data- och batterikapacitet medan Neshenko et al. (2019) uttrycker att tillverkare av IoT-enheterna inte prioriterar säkerhetsåtgärder för att öka intäkter. I samband med utvecklingen av IoT har det även blivit lättare att installera enheten i hemmet vilket bidragit till att fler tekniskt oerfarna användare tillkommer

(Gilchrist, 2017). Forskning visar att ansvaret för säkerhet läggs på användarna och att medvetenhet kring säkerhetsrisker hos användare är bristfällig (Neshenko et al., 2019; Streiff et al., 2019; Zwilling et al., 2022). Medvetenhet om säkerhetsriskerna inom IoT och smarta hem är en viktig aspekt och det behöver undersökas hur användare kan göras mer medvetna (Koohang et al., 2022; Neshenko et al., 2019; Rice & Bogdanov, 2019).

Samtidigt har det framförts att det är nödvändigt med ett tillvägagångssätt för att öka användarnas medvetenhet om specifikationerna IoT-enheterna innefattar samt riskerna dessa kan bidra med (Almusaylim & Zaman, 2019; Koohang et al., 2022; Rice & Bogdanov, 2019; Streiff et al., 2019). Det har identifierats att det finns olika tolkningar kring medvetenhet och vad det innefattar och att det varierar i olika kontexter (Endsley, 1995; Gross, 2013; Gutwin & Greenberg, 2002; Niemantsverdriet et al., 2019; Rice & Bogdanov, 2019). Det har även identifierats att det finns tre faser för att uppnå medvetenhet (Se tabell 1).

Tabell 1 - Faser för att uppnå medvetenhet.

Faser	Definitioner	Referenser
Uppfattning	Personer måste kunna samla in information från omgivning för att sedan välja vilken information som är relevant och inte.	Endsley, 1995; Endsley, 2001; Endsley & Garland, 2000
Förståelse	Personer måste kunna skapa sig en förståelse för informationen och med befintlig kunskap reflektera och agera.	Endsley, 1995; Endsley, 2001; Endsley & Garland, 2000
Agera	För personer ska kunna använda informationen behöver den ha en uppfattning om konsekvenser och förutse inverkan av olika beslut.	Endsley, 1995; Endsley, 2001; Endsley & Garland, 2000

I studien har det även framställts att knuffar kan användas för att influera människors omdöme, val eller beteende (Hansen, 2016; Thaler & Sunstein, 2008). Knuffar kan användas för att influera personer och underlätta vid val (Acquisti et al., 2017; Hansen, 2016; Thaler & Sunstein, 2008). Knuffar har använts inom icke-digitala områden under lång tid och ökar i användning i digitala miljöer (Mirsch et al., 2017; Schneider et al., 2018; Weinmann et al., 2016). Det finns sex designprinciper som är användbara för att vägleda människor mot bättre val (Thaler et al., 2010; Weinmann et al., 2016). Designprinciperna är: *incitament, kartläggning, standard, feedback, förväntade fel* samt *strukturkomplexa val.*

Vid knuffar behöver olika heuristiker tas hänsyn till som kan påverka personen (Schneider, 2018). Baserat ur en studie av Mirch et al. (2017) har de fyra vanligaste heuristikerna som används i digitala miljöer identifierats: framing, status quo bias, loss aversion och social norms (Se tabell 2).

Tabell 2 - Typer av heuristiker.

Heuristik	Definitioner	Referenser
Framing	Framing berör att förmedla information på ett visst sätt som influerar människor genom deras erfarenhet, värderingar och attityder.	Chong & Druckman, 2007; Lehner et al., 2016; Mirsch et al., 2017
Status quo bias	Status quo bias innefattar att människor vill vara i samma situation som tidigare vilket kan användas vid förvalda alternativ.	Acquisti et al., 2017; Mirsch et al., 2017; Thaler & Sunstein, 2008
Loss aversion	Loss aversion berör att människor värdesätter det de har och undviker hellre en förlust än erhåller en vinst.	Acquisti et al., 2017; Mirsch et al., 2017; Thaler & Sunstein, 2008
Social norms	Social norms grundas i att personer påverkas av andras beteenden och val.	Mirsch et al., 2017; Thaler & Sunstein, 2008

3 Metod

I detta avsnitt beskrivs metodansatsen, litteraturstudien och hur utformningen av prototyp har gått tillväga. Avsnittet beskriver även hur utvärdering och datainsamling utförts samt hur insamlad empiri analyseras. Slutligen tas etiska aspekter upp och metoddiskussion.

3.1 Metodansats

Studiens syfte är att besvara forskningsfrågan *Hur kan digitala knuffar designas för att stödja användares medvetenhet kring IoT-säkerhetsrisker i smarta hem?* För att besvara forskningsfrågan har en designorienterad forskningsansats tillämpats då metoden används för att skapa en förståelse och generera kunskap genom en prototyp (Hevner et al., 2004). En designorienterad forskningsansats fokuserar på att utforska problemområdet genom skapandet samt utvärderingen av prototyp som kan bidra till en djupare förståelse för ett identifierat problem samt generera ytterligare kunskap (Hevner et al., 2004; Zimmerman & Forlizzi, 2014). I studien användes en prototyp som utvärderades med testpersoner för att undersöka hur olika designförslag kan stödja medvetenhet kring säkerhetsrisker i det smarta hemmet.

Genom att ta fram innovativa lösningar, utvärdera och utforska lösningar på olika problem kan designorienterad forskningsansats generera ny kunskap (Hevner et al., 2004). En designorienterad forskningsansats har varit lämplig att använda till studien då prototypen möjliggjorde för att testa hur digitala knuffar kunde stödja testpersonernas medvetenhet om säkerhetsrisker. Ett kvalitativt tillvägagångssätt möjliggör för att uppfatta den sociala verkligheten och det som händer i den på samma sätt som deltagarna (Bryman, 2018). På grund av att studien har undersökt hur användares medvetenhet påverkas har en kvalitativ strategi varit relevant.

Studien bestod av en litteraturstudie som följdes av prototyputveckling som slutligen utvärderades. Litteraturstudien bidrog till en djupare förståelse för problemområdet och lade grunden för de olika designelement som implementerades i prototypen. Litteraturstudien låg även som grund för definition av medvetenhet och hur det uppnås. Prototypen som skapades baserades på de olika heuristiker samt designprinciper som identifierades under litteraturstudien. Dessa designelement utvärderades sedan för att studera hur digitala knuffar kan designas för att stödja medvetenhet kring IoT-säkerhetsrisker i smarta hem. För utvärderingen har faser för att uppnå medvetenhet som identifierades ur litteraturstudien använts: uppfattning, förståelse och agera. Vid utvärderingen användes en kvalitativ metodansats eftersom det bidrar till en fördjupad förståelse för forskningsområdet samt testpersonernas upplevelser i det specifika sammanhanget (Bryman, 2018).

3.2 Litteraturstudie

För att skapa en god översikt över det aktuella studieområdet har en narrativ litteraturstudie genomförts. En narrativ litteraturstudie innebär en granskning av existerande forskning som bidrar till en överblick över det aktuella forskningsområdet, vad som redan är känt, motsättningar och centrala begrepp (Bryman, 2018). Genomgående under litteraturstudien har databaserna Scopus och Google Scholar använts. En övergripande litteraturstudie inleddes för att ta fram relevanta begrepp och nyckelord som sedan användes för att en efterföljande smalare litteraturstudie. Nyckelorden som användes vid den första övergripande litteraturstudien var: *internet of things*, *nudge* och *security.* Från den smalare sökningen identifierades sedan nyckelorden *awareness, digital nudge* och *smart home.*

Vid den smalare litteraturstudien har samtliga nyckelord använts i kombination med varandra samt har framåt- och bakåtsökningar utförts. Framåt- och bakåtsökningar möjliggör för att hitta artiklar som kan vara av relevans till forskningsfrågan (Webster & Watson 2002). För bakåtsökningar användes referenslista ur de funna artiklarna och för framåtsökningar användes citeringsindex ur databaser. Detta resulterade i att fler artiklar, böcker och undersökningar identifierades. Litteraturens relevans och användbarhet till studien har bedömts utifrån vilket forskningsområde som behandlats, nyckelord, vetenskaplig granskning och antal citationer. Den slutgiltliga litteraturstudien resulterade i 38 artiklar.

3.3 Prototyp

Studien har ämnat att undersöka hur digitala knuffar kan designas för att stödja användares medvetenhet om säkerhetsrisker. För att undersöka detta har en prototyp med olika designelement framställts vilket har testats med användare för att sedan utvärderas. En prototyp är ett användbart verktyg som kan användas till att utforska idéer och testa dessa med användare för att ta fram ny kunskap (Hevner et al., 2004). Prototyper kan användas för att utforska designidéer och bidrar till reflektion (Preece et al., 2019). Prototypens grundläggande utseende baserades ur SmartThings, en app med över en halv miljard nedladdningar som möjliggör för att hantera och kontrollera smarta enheter i hemmet (Google play, 2022). Då syftet med prototypen inte var att skapa en helt funktionell och färdig produkt har det huvudsakliga fokuset varit på hur testpersonerna reflekterade över de olika designelementens samt hur de kunde stödja medvetenhet. Vid prototypskapande bör fokus ligga på de delar som är menade att utvärderas (Lim et al., 2008). Prototypen fokuserade på användbarhet och ett avskalat utseende för att möjliggöra fokus på de element som var av intresse för att besvara forskningsfrågan (Se bilaga 4). Designelement som inte är menade att utvärderas är ändå viktiga då det kan påverka användares tankesätt kring

prototypens användningsområde (Lim et al., 2008). Den utvecklade prototypen består av fyra olika digitala knuffar som utgår från heuristiker och designprinciper för digitala knuffar som identifierades i litteraturstudien (Se tabell 2). Prototypens utformning är även viktig då den ligger som grund till hur utvärderingen går tillväga och dess resultat (Lim et al., 2008). För studiens syfte valdes därför att utforma en prototyp för mobila enheter då mobiltelefoner är vanligt förekommande vid smarta hem.

3.4 Utvärdering

3.4.1 Datainsamling

För att samla in data utfördes 10 utvärderingstester med efterföljande semistrukturerade intervjuer. Till studien utvärderades prototypen avseende hur digitala knuffar kan stödja användares medvetenhet kring IoT-säkerhetsrisker i smarta hem. En utvärderingsmetod är att studera artefakten efter vissa kvaliteter, exempelvis användbarhet (Hevner, 2004). Utvärdering är en betydande del i forskningsprocessen och inför utvärdering behövs lämpliga kriterier fastställas (Hevner, 2004).

Utvärderingstesterna gjordes på distans via Teams och spelades in för att senare kunna transkriberas. Inför utvärderingstestet lästes ett talarmanus upp som innehöll studiens syfte, datahantering samt informera deltagaren om de skulle uppleva tvång kan de avbryta studien (Se bilaga 1). Det presenterades även ett scenario om prototypen samt att deltagaren kommer få uppgifter under utvärderingens genomförande (Se bilaga 2). Scenarios kan beskriva kontexten, målen samt aktiviteterna som användaren utför och används för att utforska ett perspektiv av en produkt (Preece et al., 2019). Scenariot förklarade prototypen och bidrog till att testpersonerna enklare kunde sätta sig in i situationen och skapa underlag för diskussion. Detta utfördes genom att förklara prototypens bakgrund till varför användaren har installerat prototypen, dess syfte samt vad dess funktioner kan användas för.

Under utvärderingstesterna användes think-aloud metoden. Think-aloud är ett bra sätt för att förstå hur en annan människa tänker (Preece et al., 2019). Metoden möjliggjorde för att samla in testpersonernas resonemang och tankar samtidigt som det öppnade upp för frågor.

Efter utvärderingstestet utfördes semistrukturerade intervjuer. Semistrukturerade intervjuer består av ett antal förbestämda frågor men möjligheten att ställa frågorna i olika ordningsföljd samt ställa fler frågor vid behov som inte är bestämda (Bryman, 2018). För studien var det viktigt att förstå testpersonernas ståndpunkter samtidigt som det skulle finnas utrymme för att avvika från intervjufrågorna. Av den anledningen utfördes semistrukturerade intervjuer efter utvärderingstestet med en fastställd intervjuguide (Se bilaga 3). Intervjuguiden utformades med ett antal

standardfrågor före prototyptest med avsikt att skapa förståelse kring testpersonens bakgrund relaterat till IoT-enheter. Det utformades även frågor efter prototyptest med öppna frågor. De öppna frågorna var dels kring hur prototypen upplevdes i helhet samt hur vardera designelement upplevdes enskilt. Både frågorna kring upplevelsen av prototypens i sin helhet samt kring de vardera designelementen förhöll däremot fortfarande utrymme för att kunna ställa efterföljande frågor med syfte att studera hur och varför kring testpersonernas upplevelse.

3.4.2 Urval

Till studien användes ett målstyrt urval för att på ett strategiskt sätt välja ut relevanta testpersoner. Ett målstyrt urval möjliggör för att identifiera och få tillgång till deltagare som är av relevans för att besvara forskningsfrågan (Bryman, 2018). Urvalskriterierna som användes för att välja testpersoner var att de skulle vara över 18 år och ha IoT-enheter i uppkopplade i hemmet. Eftersom utvärderingen genomfördes digitalt var studien inte geografiskt begränsad vilket möjliggjorde för ett bredare urval. I studien deltog 10 personer med olika bakgrund, kön och ålder (Se tabell 3). För att identifiera relevanta personer till studien lades ett inlägg ut i en Facebook-grupp med fokus på IoT. Inlägget efterfrågade om det fanns medlemmar som kunde delta i studien. Det kontaktades även bekantas bekanta som uppnådde urvalskriterierna. För att säkerställa att testpersonerna förblir anonyma har pseudonymer använts i form av siffror. Deltagarnas kön och ålder, förutom att de var över 18 år, var inget kriterium men presenteras i studien för transparens.

Tabell 3 - Testpersoner.

Testperson	Kön	Ålder	Intervjulängd
1	Man	56	37 minuter
2	Kvinna	22	30 minuter
3	Man	25	56 minuter
4	Man	56	37 minuter
5	Man	58	38 minuter
6	Kvinna	43	34 minuter
7	Man	23	30 minuter
8	Man	22	35 minuter
9	Man	29	31 minuter

10	Kvinna	24	38 minuter

3.4.3 Pilotstudie

Innan utvärderingstesterna utfördes en pilotstudie. Målet med en pilotstudie är att undersöka om någonting behöver ändras innan den riktiga undersökningen utförs (Bryman, 2018). Till studien var pilotstudiens syfte att granska om något med scenariot, prototypen eller intervjuguiden behövde tydliggöras. Pilotstudien utfördes med en person som uppfyller urvalskriterierna och som inte deltog under de senare testerna då resultatet kan bli skevt till följd av det. Under pilotstudien framkom det att prototypen upplevdes som visuellt tilltalande och användarvänlig. Intervjufrågornas ordningsföljd behövde itereras då den ordningsföljden ansågs ologisk och följde inte en röd tråd. Det gjordes även små ändringar i frågornas formulering då en del syftningsfel identifierades.

Pilotstudien visade även att när vissa frågor ställdes som tillhörde till vissa designelement ville testpersonen klicka tillbaka till det specifika designelementet. Därav kopplades prototypen att alltid möjliggöra för testpersonen att gå tillbaka till start för att kunna se de individuella designelementen igen i sitt ursprungsstadie. Detta möjliggjorde för användaren att läsa text och gå igenom vissa moment igen för att lättare kunna reflektera över och besvara frågor. Pilotstudien bidrog även med en ungefärlig utvärderingstid runt 45 minuter som var användbar för att kunna ge framtida testpersoner en uppskattad tidsram för utvärderingstest.

3.4.4 Analysmetod

Studiens syfte har varit att undersöka hur digitala knuffar kan designas för att stödja användares medvetenhet om IoT-enheters säkerhetsrisker i ett smart hem. För att undersöka detta har en kvalitativ metod använts. En kvalitativ metod är användbar för att bryta ner stor mängd data för att göra den mer hanterbar och möjliggör för att koda, organisera och identifiera samband samt mönster som kan vara till användning för studiens frågeställning (Fejes & Thornberg, 2019). Samtliga utvärderingstester och intervjuer har spelats in med inspelningsutrustning och sedan transkriberats. Inspelning möjliggör för att granska materialet igen vid behov medan transkriberingen underlättar för en mer noggrann analys (Bryman, 2018).

För att analysera resultatet av utvärderingstesterna valdes att utföra tematisk analys. I en tematisk analys kodas och kategoriseras insamlad data baserat på likheter och skillnader för att reducera och strukturera stor mängd data (Fejes & Thornberg, 2019). Det insamlade datan summerades genom kodning av nyckelord eller korta meningar. Dessa koder samlades sedan

efter de utvärderingskriterierna som tidigare identifierades i litteraturstudien avseende de faser som behövs för att uppnå medvetenhet (Se tabell 1).

I början användes utvärderingskriterierna, *uppfattning*, *förståelse* och *agera* som kategorier. Därefter sorterades koderna efter vilken kategori de ansågs tillhöra. Efter att samtliga koder sorterats granskades de efter liknande mönster och samband. De koder som upplevdes tillhöra varandra sammanställdes sedan till teman. Till uppfattning framkom temat *visuell representation* med underliggande teman *färg* och *form.* Till förståelse uppstod teman *konsekvenser* samt *statistik*. Slutligen till agera uppstod teman *komplexitet* samt *funktionalitet.*

3.5 Etiska aspekter

Eftersom studien involverar personer har det varit viktigt att följa etiska principer. Under studien har grundläggande etiska frågor som rör frivillighet, integritet, konfidentialitet och anonymitet tagits till hänsyn. Studien har även förhållit sig till de fyra forskningsetiska principerna: informationskravet, samtyckeskravet, konfidentialitetskravet samt nyttjandekravet (Bryman, 2018). Inför varje utvärderingstest har ett talarmanus lästs upp som innefattar studiens syfte och bakgrund samt hur datan kommer användas och hanteras (Se bilaga 1). I talarmanuset blev testpersonen även informerad att de kan avbryta sin medverkan utan att behöva ange anledning.

3.5.1 Informationskravet

Informationskravet behandlar att deltagaren ska bli informerad kring studiens syfte, att det är frivilligt samt att deltagaren har rätt att avbryta sitt deltagande utan att ange skäl (Bryman, 2018). Deltagarna informerades om att deras deltagande är frivilligt och vad deras deltagande i studien innebar.

3.5.2 Samtyckeskravet

Samtyckeskravet är ett krav på att deltagarna ska lämna samtycke till att delta i studien samt ha bestämma själva över sin medverkan (Bryman, 2018). Även om samtycke har lämnats ska det inte finnas tvång eller krav under studien (Bryman, 2018). Deltagarna upplystes att om de inte längre ville delta i studien av någon anledning kan kan behöver de inte gör det.

3.5.3 Konfidentialitetskravet

Konfidentialitetskravet innebär att uppgifter om deltagarna som ingår i studien ska behandlas med största möjliga konfidentialitet (Bryman, 2018). Personuppgifter och andra uppgifter ska behandlas på ett sådant vis som gör

det omöjligt för utomstående att identifiera enskilda personer. Vidare ska även de insamlade uppgifterna förvaras på ett säkert vis som utomstående inte kan få tillgång till. Personuppgifter, ljud- och bildinspelningar har lagrats på en hårddisk för att obehöriga ej ska ha möjlighet att få tillgång till materialet.

3.5.4 Nyttjandekravet

Nyttjandekravet innefattar hur uppgifter som samlas in om enskilda personer används. Det får endast användas för forsknings ändamålet och inte delas med utomstående (Bryman, 2018). De uppgifter som samlas in ska enbart användas till studien och får endast delas med tredje part med medgivande från berörd person (Bryman, 2018). Den data som samlats in har endast använts för studiens syfte och samtliga personer som deltagit i studien har anonymiserats genom pseudonymer.

3.6 Metoddiskussion

Forskning borde ha som mål att uppnå en hög kvalitet (Bryman, 2018). För forskning att uppnå en hög grad av kvalitet kan det vara av vikt att den kvalitativa forskningen berör ett relevant tema (Tracy, 2010). För att ett tema ska vara relevant behöver det vara aktuellt, intresseväckande eller betydelsefullt på något vis (Tracy, 2010). Under litteraturstudien har det identifierats att det finns en brist på medvetenhet hos användare kring IoT-säkerhetsrisker i det smarta hemmet (Neshenko et al., 2019; Streiff et al., 2019; Yang et al., 2017). Genom att undersöka hur digitala knuffar kan designas för att stödja medvetenhet kring säkerhetsrisker kan personer vara mer medvetna om potentiella risker. Dessa risker kan ha stora konsekvenser för användare och det finns inte tillräckligt med tillvägagångsätt för att upplysa eller förebygga dessa (Almusaylim & Zaman, 2019; Koohang et al., 2022; Rice & Bogdanov, 2019; Streiff et al., 2019). Det finns tre faser för att uppnå medvetenhet (Endsley, 1995; Endsley, 2001; Endsley & Garland, 2000). Dessa faser har använts som utvärderingskriterier till studien.

Inom kvalitativ forskning är det viktigt att kunskapsbidraget är meningsfullt (Tracy, 2010). Studien har utförts med en kvalitativ ansats som kan ha påverkat studiens resultat. Bryman (2018) skriver att kvalitativ forskning ofta är subjektiv då den reflekterar forskarnas egna uppfattning som kan påverka utkomsten av studien till skillnad från kvantitativ forskning. En kvalitativ metod möjliggör dock för att prata med människor och fånga deras tankar, känslor och upplevelser (Bryman, 2018). Till studien har den kvalitativa metoden varit lämplig att använda då det har möjliggjort för att utvärdera medvetenhet som inte kan mätas i samma grad med en kvantitativ ansats.

Urvalet till studien har varit fokuserad på personer som kan bidra till att besvara forskningsfrågan. Urvalet vid en kvalitativ studie ska reflektera den variation som finns inom forskningsområdet (Bryman, 2018). Utvärderingarna har utförts med personer som har tillgång till IoT-enheter i hemmet och är över 18 år gamla. Under urvalet var det eftertraktat att uppnå en jämn fördelning mellan könen däremot i slutändan blev majoriteten av urvalet män. Däremot bör studiens urval inte påverkat resultatet då litteraturstudien identifierade att det inte var skillnad mellan kvinnor och män avseende medvetenhet om säkerhetsrisker.

För att beröra så många parter som möjligt bör urvalet vara jämlikt med den variation som finns inom forskningsområdet (Bryman, 2018). Till studien hade testpersonerna olika grad av erfarenhet och teknisk kunskap för att matcha den variation som finns. Om studien skulle ha undersökt testpersoner baserat på deras tekniska erfarenhet kan resultatet varierat, detta är något som kan vara av intresse att undersöka i framtida studier. Vid studiens genomförande uttryckte testpersonerna 4 och 6 att de hade mer erfarenhet och kunskap om säkerhet kring IoT än i jämförelse med en vardaglig användare. Trots detta framhävs fortfarande likartade reflektioner som resterande testpersoner. Den skillnaden som framhävdes vid resultatet var att de mer tekniskt erfarna reflekterade kring sin egna kunskap om säkerhet och var mer skeptiska till vad designelementen knuffade åt.

Under studien har kvalitativa intervjuer utförts som möjliggjorde för att förhålla flexibilitet genom att ställa följdfrågor samt tydliggöra om testpersonerna inte förstår. Det har samtidigt bidragit med insikter avseende vad det är som testpersonerna anser är viktigt. Detta adaptiva tillvägagångssätt hade inte varit möjlig vid en kvantitativ ansats.

Utvärderingarna på datorn utfördes med Figma som möjliggjorde för testpersonerna att använda en virtuell mobiltelefon som styrdes med hjälp av muspekaren. Det bidrog även till att utvärderingarna kunde utföras på distans och inte var begränsade av en specifik mobiltelefon modell. Föredraget hade varit att utföra testerna på mobil på distans men det skulle bli mer invecklat för testpersonerna att dela skärm på en mobiltelefon samtidigt som de testade prototypen. Samtidigt har studien ämnats att utforska att testa de olika designförslagens stödjande av medvetenhet, inte hur de fungerade på dator eller mobil.

4 Designstudien

Under designstudien tas problemidentiferingsfasen upp som sedan leder in på hur de olika designelement skapades. Det redogörs för hur de olika heuristikerna och designprinciper för design av digitala knuffar har använts vid designelementen samt hur de utvärderas mot definition av medvetenhet.

4.1 Problemidentifieringsfas

Det argumenteras för att det är nödvändigt att skapa ett tillvägagångssätt för att öka medvetenheten avseende säkerhetsriskerna som finns i IoT-enheter (Ando et al., 2016; Rice & Bogdanov, 2019). Det finns flertal olika anledningar till säkerhetsrisker inom IoT. Dels är det för att det saknas medvetenhet hos användare då säkerhetsriskerna inte är tydliga (Streiff et al., 2019). Att de implementerade säkerhetsfunktionerna är bristfälliga (Almusaylim & Zaman., 2019). Det beror även på att det är svårt för användare att identifiera hoten (Kraemer et al., 2009; McDermot et al., 2019).

Genom knuffar kan personers omdömen, beteenden och val påverkas genom kognitiva funktioner fördomar, rutiner och vanor (Hansen, 2016). Studien har ämnat att undersöka och utvärdera hur digitala knuffar kan designas för att stödja IoT-användares säkerhetsmedvetenhet i smarta hem. Knuffar har använts inom flera olika områden tidigare men inom informatik och digitala sammanhang har det inte undersökts lika mycket (Mirsch et al., 2017; Schneider et al., 2018; Weinmann et al., 2016).

Utvärderingen har genomförts med en prototyp bestående av fyra olika designelement relaterat till olika designprinciper samt heuristiker som framing, status quo bias, loss aversion och social norms (Se tabell 4).

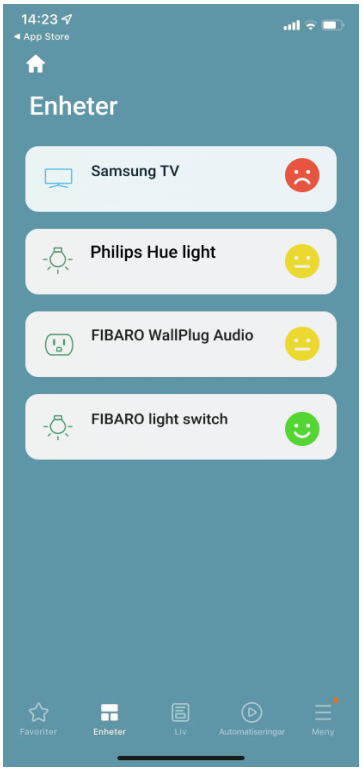
Tabell 4 - Översikt över designelement som tillämpas i prototypen samt vilka heuristiker och designprinciper de utgår från.

Designelement	Heuristiker	Designprinciper
Designelement 1: Säkerhetsstatus	Framing	Strukturkomplexa val, Kartläggning
Designelement 2: Automatiska uppdateringar	Status quo bias	Standard
Designelement 3: Varningsmeddelande	Loss aversion	Feedback
Designelement 4: Social påverkan	Social norms	Kartläggning, Standard

4.2 Designfas

4.2.1 Designelement 1: Säkerhetsstatus

Framing kan bidra till att personer tar bättre beslut och kan användas för att förmedla information till personer genom erfarenhet, värderingar och attityder (Chong & Druckman, 2007; Lehner et al., 2016; Mirsch et al., 2017). Framing kan användas för att presentera information positivt eller negativt (Thaler & Sunstein, 2008). Till Designelement 1: Säkerhetsstatus har tre olika smileysar i olika färger använts för att göra användaren upplyst om hur allvarliga risker det kan finnas på de uppkopplade IoT-enheterna i hemmet. Att möjliggöra för användare att tolka information baserat på erfarenheter och kunskap tillåter för att förstå information bättre (Weinmann et al., 2016). Anledningen varför smileysar och färger har implementerats är på grund av designprincipen *kartläggning,* vilket innefattar att få människor att tolka information baserat på tidigare erfarenheter (Weinmann et al., 2016). Färgerna som användes var röd, gul och grön där röd representerar stora säkerhetsrisker, gul representerar medelmåttiga säkerhetsrisker och grön representerar att det inte finns några säkerhetsrisker. Anledningen till att dessa färger används samt varför de representerar olika grader av säkerhetsrisker är på grund av att de ofta används i liknande syfte, trafikljus, varningsskyltar, digitalt kodlås etcetera. Att tillåta för personer att jämföra olika val kan möjliggöra för att göra avvägningar vid *strukturkomplexa val* när det är nödvändigt (Thaler et al., 2010; Weinmann et al., 2016). Till Designelement 1: Säkerhetsstatus används designprincip *strukturkomplexa val* för att visa användaren komplex information på ett hanterbart vis genom färg och form. Smileysarna har även utformats med olika humör för att ytterligare symbolisera enheternas säkerhetsstatus. Glad för att representera inga säkerhetsrisker, neutral för att representera medelmåttiga säkerhetsrisker och ledsen smiley för att representera stora säkerhetsrisker.



Figur 1 - Designelement 1: Säkerhetsstatus.

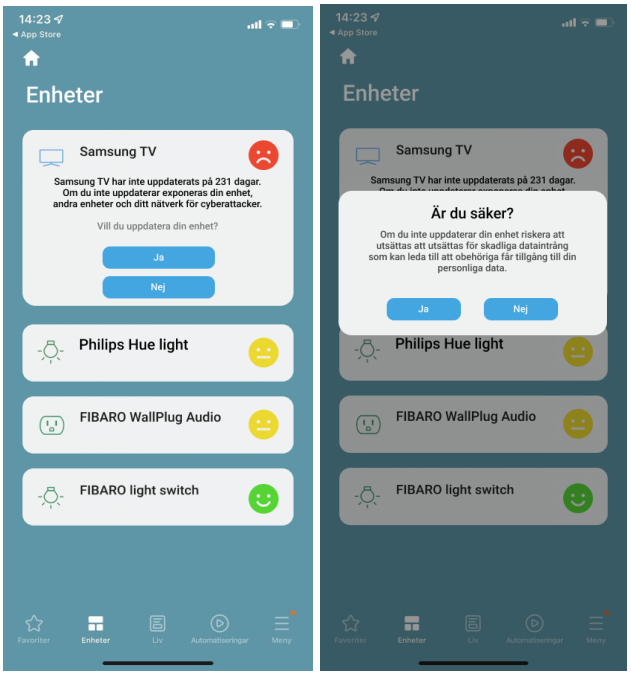
4.2.2 Designelement 2: Automatiska uppdateringar

Vid Designelement 2: Automatiska uppdateringar implementerades information om fördelar med att aktivera automatiska uppdateringar och ett förinställt alternativ för att aktivera presenterades. Det förinställda alternativet behandlade designprincipen *standard* som innebär att presentera förvalda alternativ då personer har en tendens att inte ändra dessa (Weinmann et al., 2016). Status quo bias innefattar att användare är ouppmärksamma och klickar på det förvalda alternativet då det förvalda alternativet anses vara det bästa alternativet (Thaler & Sunstein, 2008). De automatiska uppdateringarna leder till att användarens enheter och nätverk är säkrare än vad de annars skulle vara. För att knuffa användaren åt att aktivera automatiska uppdateringar är alternativet att aktivera automatiska uppdateringar förinställt. Att presentera förvalda alternativ kan vara gynnsamt för att leda personer mot bättre valalternativ (Weinmann et al., 2016). Status quo bias kan vara användbart för att underlätta beslutstagande och knuffa personer åt bättre valalternativ (Thaler & Sunstein, 2008).

Figur 2 - Designelement 2: Automatiska uppdateringar.

4.2.3 Designelement 3:Varningsmeddelande

Loss aversion innebär att personer hellre erhåller en vinst är vara med om en förlust (Acquisti et al., 2017; Thaler & Sunstein, 2008). För loss aversion kan information presenteras genom att få användare att känna att de förlorar om de inte utför ett val nu (Mirsch et al., 2017). Designelement 3: Varningsmeddelande består av informerande text som visar på konsekvenser av att inte uppdatera en enhet. Ytterligare presenteras information i ett popup-fönster med ytterligare negativa konsekvenser om enheten inte uppdateras. Detta för att skapa en känsla av att förlora något om valet inte tas. Detta implementerades i hänsyn till designprincip *feedback* som behandlar att informera användare baserat på vilka val de gör (Weinmann et al., 2016). Att ge återkoppling kring olika val kan bidra med en uppfattning om ett valalternativ är bättre eller sämre än ett annat val (Weinmann et al., 2016). Designelement 3: Varningsmeddelande knuffar åt att tänka över beslut och göra användaren mer medveten om konsekvenser av val. Loss aversion kan användas för att underlätta beslutsprocessen och göra det lättare att ta fördelaktiga val (Mirsch et al., 2017).



Figur 3 - Designelement 3: Varningsmeddelande.

4.2.4 Designelement 4: Social påverkan

Social norms innefattar att människor agerar efter samma beteende som andra människor (Mirsch et al., 2017). I Designelement 4: Social påverkan visar information om hur andra användare valt att gå tillväga angående att koppla ifrån en osäker enhet. Att presentera information, statistik eller text om hur andra agerat kan underlätta val (Hansen, 2016). Statistik i Designelement 4: Social påverkan visar att fyra av fem användare valt att frånkoppla den osäkra enheten och uppmanar till att frånkoppla för att öka säkerheten. I designelementet har designprincipen *kartläggning* samt *standard* använts genom att framhäva information som är bekant till användaren samt indikera vad användare bör göra baserat på andras utförande (Weinmann et al., 2016). Genom att använda information avseende hur andra människor utför val kan detta användas för att influera nästa persons val (Thaler & Sunstein, 2008). Designelement 4: Social påverkan grundas i att människor har en tendens att inte vilja bryta den sociala normen. Andras agerande påverkar beslut och gör personer mer medveten om sina val.

Figur 4 - Designelement 4: Social påverkan.

4.3 Utvärderingsfas

Under studien utfördes totalt 10 utvärderingstester som spelades in och transkriberades för att möjliggöra att enklare analysera materialet. Datan som framställdes under utvärderingsfasen samlades undertill utvärderingskriterierna för att uppnå medvetenhet: uppfattning, förståelse och agera. Detta assisterade att koppla teman som uppstod under utvärderingsfasen till olika faser av medvetenhet. Tillhörande uppfattning identifierades temat *visuell presentation* med underliggande teman, *färg* och *form*. Under förståelse identifierades teman *konsekvenser* samt *statistik*. Under agera identifierades två teman, *komplexitet* samt *funktionalitet*. Samtliga teman som identifierades under analys av material redovisas och ligger som grund för diskussion och konceptionalisering.

4.3.1 Uppfattning

Visuell representation

Utvärderingarna visade att testpersonerna uppmärksammade de färgglada smileysarna i prototypen och kopplade att de relatera till enheternas säkerhetsstatus. Samtliga testpersoner uttryckte att den ledsna röda smileyn representerade hög allvarlighetsgrad och den glada gröna smileyn representerade ingen allvarlighetsgrad. En del av testpersoner tolkade att gul neutral smiley indikerade att enheten var osäker medans andra testpersoner uttryckte att det behövde tydliggöras. Däremot framkom det att de inte

förstod varför enheterna hade den säkerhetsstatus som de hade. Genom tematiseringen identifierades att testpersonerna tolkade att det var *visuell representationen* som indikerade enheternas säkerhetsstatus. *Visuell representation* delades upp i ytterligare två teman till *färg* och *form* baserat på vad testpersonerna uttryckte att de uppmärksammade. *Form* indikerade smileysarna avseende om den var glad, neutral eller ledsen medan *färg* indikerade de färger som smileysarna var ifyllda, grön, gul eller röd. Testpersonerna blev tillfrågade om de skulle förstå enheten status med enbart smileysarna eller med enbart färg. Samtliga uttryckte att enhetens status kunde tolkas med *färg* enskilt eller med *form* enskilt men att det skulle vara mindre tydligt och därmed ta längre tid. De uttryckte att de två elementen i kombination med varandra var tydligast för att få en uppfattning om enhetens säkerhetsstatus. Digitala knuffar som använder färg och form i kombination med varandra stödjer användarens förståelse avseende hur säker en IoT-enhet är.

"*Även om smileysarna inte haft färg tror jag ändå att jag skulle förstått men färgerna uppmärksammade jag var extra tydliga.*" - Testperson 7

"*Kanske efter ett tag. Men det hade tagit längre tid att förstå vad de betyder. Kombinationen gör att det är supertydligt*." - Testperson 2

"Om de hade varit färglösa tror jag man hade förstått men de är tydligare med färg." - Testperson 3

Testpersonerna uttryckte att färg och form är ett tydligt sätt att få information på och att de kan relatera olika färger och former från sammanhang i verkligheten, som exempelvis trafikljus. Det diskuteras dock att i nya sammanhang kan det vara användbart att använda både färg och form för att förtydliga. Testpersonerna relaterade visuell representation till sin vardag och kunde därmed tolka information effektivare. Röd färg indikerade fara och en glad smiley indikerade positiv representation exempelvis.

Visuell representation - Form

Flera av testpersonerna uttryckte att smileysarna var bra för att visa enheternas status och skapa en förståelse för att något behöver uppmärksammas. Det argumenteras för att smileysarna är tydliga och kan lätt tolkas som att något är bra eller dåligt beroende på om den var ledsen, neutral eller glad.

“När det är en gubbe som har olika utseende så kan du lätt se att något står på tok. Jag hade nog valt att se den med ledsen gubbe först för det verkar vara något fel på den.” - Testperson 5

“Dom är bra, mycket vedertagna. Plus för dom. Det var det första jag tänkte att här finns det hög säkerhetsrisk, här lägre och så vidare.”
- Testperson 1

Trots att testpersonerna uttryckte att de upplevde att smileysarna gav inblick över de olika enheternas säkerhetsstatus saknades information angående vad som är fel på enheten. Det visar även på att smileysarna inte är tydliga med att representera varför den har det ansiktsuttryck den har och vad det baseras på. Det finns ett behov för ytterligare information över de olika tillstånden hos smileysarna för att tolka de mer tydligt.

“Smileysarna visar att det är ett problem men inte vad problemet är.”
- Testperson 2

“Jag förstår att smileysarna symboliserar säkerhetsrisk. I min åsikt är det lite vagt, jag vill gärna veta varför det är en ledsen smiley, varför har den det betyget.” - Testperson 7

Det diskuterades även om olika former kunde ha samma effekt som smileysar och en del av testpersonerna argumenterar för att ett kryss eller checkmärke kan skapa uppfattning.

"Om man hade haft haft ett kryss på den röda, en checkmark på den gröna och ett streck på den röda hade man förstått också.” - Testperson 8

Visuell representation - Färg

Under studien framhävdes testpersonerna att färgkombinationen rött, gult och grönt var tydliga då de är vanligt förekommande i samband där status representeras i dessa olika *färger*. En del av testpersonerna relaterade *färgerna* till trafikljus medan andra relaterade den röda *färgen* till brand eller fara och ansåg därmed att enhetens status framfördes på ett effektivt vis. Gemensamt uttryckte testpersonerna att den röda *färgen* var den som

indikerade högst säkerhetsrisk, att gul var medel och att den gröna *färgen* framhävde att enheten var säker.

"Smileysarnas färger påminner om trafikljus, jag tycker det är väldigt tydligt." - Testperson 8

"Ja, första gången jag går in på appen så rör sig mina ögon mot de röda färgerna. Jag känner att jag behöver släcka bränder först liksom."
- Testperson 7

"Alla vet vad färgerna betyder, röd är panik, gul är varning och grön betyder okej." - Testperson 4

Likt resonemanget om olika formers betydelse framkom det att att många tolkade de olika *färgerna* likartat men att behövdes mer information avseende varför enheterna hade den *färg* de hade. Majoriteten av testpersonerna uttryckte att de kopplade *färgernas* betydelse till säkerhetsrisken däremot framkom en osäkerhet kring den gula färgen då den inte framhävde tydligt att de enheterna var osäkra. Testpersonerna höll med om att *färgerna* var tydliga för att skapa en uppfattning om enheternas olika säkerhetsstatus men att det kan behöva förklaras ytterligare.

"Funderade lite över de gula smileysarna, vet inte riktigt hur jag ska tolka de. Är det värt att bry sig om dom eller inte? Om de är röda skulle jag nog var mer benägen att koppla ifrån eller göra saker för att höja säkerheten."
- Testperson 10

4.3.2 Förståelse

Statistik

Vid utvärderingen utsattes testpersonerna för ett val om att stänga av en enhet som inte var säker eller lämna den påslagen. Prototypen presenterade information angående hur andra användare agerat och visade att fyra av fem användare valt att frånkoppla enheten. Att få information om hur andra valt att göra skapade en förståelse avseende enheternas säkerhetsstatus. Genom tematiseringen framhävdes det att *statistik* influerade testpersonerna. Hälften av testpersonerna valde att stänga av enheten på grund av att andra användare gjort det. Även fast den andra hälften inte stängde av enheten

reflekterade de över enhetens säkerhetsstatus och om det var något annat de kunde göra för att få enheten mer säker.

"Jag tänkte att oj, om 80% kopplar ifrån borde inte jag vara en av dom som inte gör det? Är det jag som missat någonting?" - Testperson 3

"Jag tänker att någon annan av dessa har läst på att det är bättre att koppla bort enheten. Beroende på enhet kanske jag undersöker mer vad riskerna kan vara." - Testperson 1

Utvärderingsfasen framhävde däremot att vissa av testpersonerna menade att *statistiken* var påträngande. På grund av att andra användare hade stängt av enheten upplevdes *statistiken* som ett tvång att de själva också bör stänga av den.

"Det var det med att jag tyckte det var lite vinklat och jag kände mig lite tvingad att också göra det. Jag tolkade det som att man ska göra det, eftersom majoriteten valt att göra det." - Testperson 6

"Lite grupptryck känsla kanske. Om man utgår ifrån att de som gjort detta valet gjorde det för att de är kunniga påverkas jag ju."
- Testperson 9

Testperson 4 och 6 som beskrev att de hade mer kunskap inom säkerhet kring IoT än en vardaglig användare uttryckte att statistiken om hur andra agerat inte påverkade dem. Istället berättade de att de inte hade stängt av enheten direkt utan undersökt enhetens säkerhetsrisker ytterligare för att sedan ta ett beslut. På grund av deras kunskap inom området ansåg de att andras agerande inte nödvändigtvis är det bästa alternativet.

"Jag tror inte att det påverkar mig för att det är inte alltid det som alla andra gör som är det bästa alternativet. Jag hade kopplat bort den för det är en risk men inte för att andra gjort det." - Testperson 6

"Nej, jag känner inte att jag kan lita på den infon. Vilka är dessa? Vad vet de och och vad är deras bakgrund? Jag vill hellre gå till den specifika enheten och lösa problemet där. Jag tycker det är pöbel argumentation att andra gjort så." - Testperson 4

Konsekvenser

I ett utfall om testpersonerna valde att ha en osäker enhet uppkopplad presenterades ett popup-fönster som informerade att deras personliga data riskerar att exponeras. Många av testpersonerna som valde att lämna enheten uppkopplad uttryckte att de reflekterade över de potentiella *konsekvenser* som kunde inträffa om enheten lämnas påslagen. Flertalet av testpersonerna uttryckte även att *konsekvensen* kan ha en inverkan som leder till att de tänker till en extra gång men att det inte påverkade deras beslut i slutändan. Det framfördes att när testpersonerna blev informerade om *konsekvenserna* uppnådde de en förståelse över de potentiella säkerhetsriskerna som IoT-enheterna medför, det påverkar dock inte nödvändigtvis deras beslut.

"Jag tänker att om jag inte uppdaterar så riskerar den att bli utsatt. Det är bra för jag förstår riskerna men jag har ändå ett val om vad jag vill göra."
- Testperson 1

"Bra information, rakt på sak. Lite som texten innan men ännu lite hårdare. Lite tydligare vad konsekvenserna är om du inte kopplar bort."
- Testperson 10

"Här tycker jag det är bättre förklarat vad som händer om jag inte kopplar ifrån den. Den får mig att tänka igenom en sista gång men eftersom jag redan tryckt att jag inte vill koppla ifrån den så har jag redan bestämt mig och det krävs ganska mycket för att få mig att ändra mitt val."
- Testperson 3

När testpersonerna blev informerade genom varningsmeddelandet att en enhet var utsatt var de intresserade av att ta reda på mer konkret vad riskerna innefattar. Testpersonerna uttryckte att de ville veta mer om konsekvenserna, exempelvis om enheten kan sluta fungera eller att den blir utsatt för virus. Vissa uttryckte att de ville veta mer om säkerhetsriskerna avseende vad för risker som fanns med enheten innan de tog ett val. Beroende på hur allvarliga *konsekvenserna* var påverkade det testpersonernas agerande.

"Det beror på hotet vill jag säga. Det som är enklast för mig är att dra ut sladden men det gör ju enheten useless så att säga. Så jag hade nog först

vilja veta vad för intrång jag fått liksom eller vad för risk jag har och agerat utifrån det." - Testperson 7

"Bara utifrån den informationen jag ser på skärmen så är jag inte så orolig men hade det stått att jag får massa trojaner hade jag blivit mer nojjig. Det beror på vad för dataintrång, den här säkerhetsrisken skulle kunna leda till. Om det är så teoretiskt att ryska hackers kan höra mig laga mat hemma är jag inte så jätteorolig för det men är det så att de kan komma åt min dator sen och börja tanka ner virus och filer i datorn via den här är det ett större problem. Så jag hade velat se mer vad för dataintrång som den här säkerhetsrisken medför." - Testperson 3

4.3.3 Agera

Komplexitet

Under utvärderingarna framhävs att även fast testpersonerna förstår de potentiella säkerhetsriskerna kring IoT-enheterna var det inte självklart om de faktiskt skulle utföra nödvändiga åtgärder för att göra enheterna säkrare. När testpersonerna frågades om de hade uppdaterat Samsung TVn i verkligheten svarade majoriteten att det beror på hur *komplext* det är. Detta innefattade att många av testpersonerna uttryckte att det behövde vara enkelt att utföra säkerhetsåtgärderna annars fanns det risk för att det skulle ignoreras.

"Jag skulle hellre vilja ha en automatisk uppdatering, eller att mjukvaran gör det åt en. Om individen behöver uppdatera själv utanför appen kommer det inte att göras." - Testperson 4

"Ju mer man förenklar någonting och ju mer du kan göra på ett och samma ställe desto lättare är det göra något åt det." - Testperson 3

"Jag hade hoppats på att man kunde göra det direkt i appen. Det är aldrig roligt att uppdatera en TV så det är inte säkert att jag hade gjort det."
- Testperson 8

I samband med Philips Hue Light svarade flera av testpersonerna att de hade uppdaterat sin enhet för att öka säkerheten. En anledning till detta framkom vara på grund av att det är lätt att utföra och kräver inte mycket jobb.

Utvärderingen visade återigen att *komplexitet* är en viktig faktor och att det kan vara avgörande för att påverka agerande hos personer.

"Det är en lättnad för då slipper jag tänka på det. Jag vill gärna ha automatiska uppdateringar aktiverat. Skönt att sätta på automatik så slipper jag göra det manuellt. Manuellt vet jag ej om jag hade gjort det. Smart funktion." - Testperson 7

"Instruktionerna var bra men det vore jävligt smidigt om man kunde uppdatera från appen. Jag tror att jag inte skulle uppdatera enheten om det inte gick att göra i appen." - Testperson 8

Funktionalitet

Vid enheten Samsung TV frågades testpersonerna om de hade uppdaterat enheten i verkligheten för att göra den mer säker. Två av testpersonerna var skeptiska om de hade gjort det. Ur utvärderingen identifierades att testpersonerna värderar enhetens *funktionalitet*.

"Beror på hur TVn fungerar efter. Just nu står det inget om det men påverkas prestandan liksom? Isåfall är jag osäker." - Testperson 7

"Förmodligen inte, när jag använder TVn vill jag se på den och inte uppdatera. Om det verkligen behöver uppdateras gör jag det. Annars känns det inte nödvändigt." - Testperson 2

Under utvärderingen hade enheten Fibaro Wallplug Audio inte tillräckligt med säkerhetsåtgärder implementerade för att säkerställa att användarens data inte riskerar att exponeras. Testpersonerna utsattes då för att välja mellan att koppla ifrån enheten från nätverket eller lämna den uppkopplad. När testpersonerna utsattes för valet frågade majoriteten vad för *funktioner* enheten hade och baserade sina svar på detta. De svarade på ett likartat sätt att om de köpt enheten förutsätter det att de vill ha den uppkopplad. Återigen identifierades att testpersonerna värderade *funktionalitet* framför säkerhet. Resultatet visade att testpersonerna har en vilja att bli mer säkra men inte på bekostnad av *funktionalitet*. *Funktionerna* som en enhet bidrar med anses vara viktigare än säkerheten i de flesta fall. När risker ställs mot förlusten av *funktioner* var det flera av testpersonerna som valde att ha en utsatt enhet i utbyte mot att *funktionerna* fortfarande kunde nyttjas.

"Min förståelse för enheten är att funktionerna försvinner om den kopplas ifrån. Alltså vill jag inte bli av med funktionerna. Om enheten inte påverkas så mycket funktionellt kan jag tänka mig koppla ifrån den." - Testperson 8

"Jag hade nog istället för att koppla ifrån den direkt valt att googla lite och se om detta faktiskt är ett bekymmer. Om det visar sig att riskerna är stora kanske jag kopplar bort enheten då. Annars vill jag ju ha enheten för det den gör" - Testperson 5

"Om jag kan koppla från enheten utan att dess funktioner försämras skulle jag göra det men vill inte förlora enheten om inte riskerna är stora. Majoriteten av mina enheterna skulle jag nog välja att ha kvar."
- Testperson 3

5 Diskussion och konceptualisering

I detta avsnitt diskuteras analys och resultat från utvärderingen. Samtliga designelement tas upp och resultatet diskuteras för att sedan sammanställa designförslag för digitala knuffar för att stödja medvetenhet. Avslutningsvis sammanställs resultatet i tabell 5 som visar på de framtagna designförslag samt vad dessa innebär.

5.1 Designelement 1: Säkerhetsstatus

Framing kan användas i design för att presentera information positivt eller negativt (Thaler & Sunstein, 2008). Det kan förmedla information till människor utifrån deras värderingar, erfarenhet och attityder (Chong & Druckman, 2007; Lehner et al., 2016; Mirsch et al., 2017). Designelement 1: Säkerhetsstatus innefattade färglagda smileysar som skulle upplysa testpersonerna om enheternas säkerhetsstatus. Resultatet visade på att samtliga testpersonerna relaterade färgerna och smileysarna till olika grad av säkerhetsrisk. Om det hade varit en symbol eller färg som testpersonen inte relaterar till olika betydelser hade potentiellt den visuella representation av IoT-enheterna blivit svårtolkad eller missvisande. Det är därmed viktigt att användaren vid behov kan få förklarat vad färgerna och formerna betyder.

Kombinationen av färg och form bidrog till att testpersonerna skapade sig en uppfattning för säkerhetsriskerna. Även fast testpersonerna inte uppnådde nästkommande faser av medvetenhet, förståelse och agera, är resultatet likt studien från Turland et al. (2015) om att färgkodning kan användas för att knuffa användare. Trots att digitala knuffar, skapade genom visuell

representation, inte knuffar användaren till att förstå vad som är fel på IoT-enheten kan det användas för att knuffa mot att vilja ta reda på mer avseende varför enheterna har den säkerhetsrisk den har. Utifrån utvärderingen framställdes att *visuell representation* genom en kombination av både *färg* och *form* var det tydligaste och mest intuitiva viset för att framhäva enheternas säkerhetsstatus. Resultatet av analysen visade även på att en del av testpersonerna upplevde att färg eller formen kunde tolkas olika och det kan därför vara nödvändigt att beskriva olika färg och form betydelse.

I Japan används en förtroendestämpel för att minska användares oro och upplysa om eventuella säkerhetsrisker på nätet (Ando et al., 2016). På ett likartat sätt fungerade de färglagda smileysarna som en *visuell representation* genom *färg* och *form* för att visa enheternas säkerhetsstatus. Testpersonerna uttryckte att designelement 1: Säkerhetsstatus bidrog med uppfattning för olika enheters säkerhetsrisker men designelementet skapade inte en förståelse avseende varför enheterna var osäkra.

Utifrån diskussion framkom designförslag: *Designa för att upplysa användaren om enhetens säkerhetsstatus genom färg och form.*

5.2 Designelement 2: Automatiska uppdateringar

Status quo bias innebär att personer har ett stort behov av att förbli i samma situation och att ett förinställt alternativ kan vägleda till att ta det alternativet istället för att ändra sin situation (Thaler & Sunstein, 2008). I Designelement 2: Automatiska uppdateringar innefattade ett förinställt alternativ att aktivera automatiska uppdateringar för en enhet. För att designa för status quo bias kan valalternativen spela roll (Thaler & Sunstein, 2008). Det alternativ som Designelement 2: Automatiska uppdateringar knuffade mot angående att aktivera automatiska uppdateringar ansåg majoriteten av testpersonerna vara det mest fördelaktiga alternativet.

Trots att testpersonerna uttryckte att de hade valt alternativet oavsett och inte påverkades av knuffen är det möjligt att de påverkades undermedvetet. Anledningen är för att människor kan vara ouppmärksamma och därmed väljer förinställda alternativ (Thaler & Sunstein, 2008). Samtidigt när människor utsätts för alternativ upplever de att förvalda alternativ är de mest optimala eftersom det antas finnas en orsak till att valet är förinställt (Thaler & Sunstein, 2008). Detta påvisades i studien då flera testpersoner påpekade att de ville ha på automatiska uppdateringar. Testpersonerna menade även på att när det valet som de tänkte ta redan var förinställt bekräftade det att deras val var rätt. Det kan bero på att det förmodas finnas en anledning till att det var förinställt. Personer anser att säkerhet och integritet är viktigt men att funktioner och de positiva aspekter som IoT möjliggör också är betydelsefulla (Gilchrist, 2017; Koohang et al., 2022; Wang et al., 2018).

Detta bekräftas i studien då det förinställda alternativet ökade säkerheten men inte påverkade enhetens *funktionalitet* blev det ett naturligt val. Om det förvalda alternativet skulle förvanska enhetens *funktionalitet* kunde utkomsten av testpersonernas val potentiellt blivit annorlunda. Det uttrycktes också med hänsyn till att det inte var *komplext* att sätta på automatiska uppdateringar främjade det beslut.

Thaler & Sunstein (2008) menar att en digital knuff kan underlätta för beslutstagande och om det finns flera alternativ kan förinställda alternativ knuffa åt ett visst val. I utvärderingen var det förvalda alternativet det vanligaste att ta bland testpersonerna vilket kan grundas i att det var lätt att ta det beslutet då det var förvalt. Resultatet överensstämmer med tidigare forskning som indikerar på att personer gärna undviker att byta alternativ om ett alternativ redan är förvalt (Mirsch et al., 2017; Thaler & Sunstein, 2008).

Resultatet av utvärderingen tyder på att *komplexitet* och *funktionalitet* är två viktiga aspekter för att personer ska agera. Majoriteten av testpersonerna valde att aktivera automatiska uppdateringar men argumenterar för att det mestadels är på grund av att det var enkelt att utföra samt att det inte påverkar enhetens *funktioner*. Av den anledningen behöver dessa två aspekter tas hänsyn till vid design av digitala knuffar för att få användare att agera.

Utifrån diskussion framkom designförslag: *Designa för att göra det enkelt för användaren att utföra nödvändiga säkerhetsåtgärder och informera hur funktionerna påverkas.*

5.3 Designelement 3:Varningsmeddelande

Loss aversion innebär att personer har ett stort behov av att inte erhålla en förlust (Acquisti et al., 2017; Thaler & Sunstein, 2008). Loss aversion innefattar att information kan presenteras på ett visst sätt vilket får användare att uppleva att de förlorar om de inte utför ett val i tillfället (Mirsch et al., 2017). I designelement 3: Varningsmeddelande implementerades loss aversion genom att framhäva om inte säkerhetsåtgärder utförs kan enheten utsättas för cyberattacker och riskera att personlig data exponeras.

Undersökningen identifierade att testpersonerna värderade enhetens *funktioner* framför *konsekvenserna*. Testpersonerna beskriver även att beroende på vad för *funktioner* en enhet besitter kan *konsekvenserna* uppfattas olika allvarliga. Streiff et al. (2019) argumenterar att det är viktigt för tillverkarna att framhäva IoT-enhetens specifikationer och typer av potentiella säkerhetsrisker. Detta bekräftas i studien däremot ville vissa av

testpersonerna veta mer om *konsekvenserna* samt om det fanns något annat de kunde göra innan de tog ett beslut.

Trots att vissa uttryckte att de ville veta mer om de faktiska riskerna uppnådde Designelement 3: Varningsmeddelande fortfarande en förståelse för säkerhetsrisker hos enheterna. Om designelementet hade designats annorlunda genom att ytterligare framhäva *konsekvenserna* hade potentiellt en högre förståelse kunnat uppnås och tillräckligt för att agera.

Legg (2016) uttrycker att det är mer troligt att användare utför säkerhetsåtgärder om det inte påverkar enhetens *funktionalitet*. Det är även en stor del av IoT-användare som inte har behov att lära sig det tekniska eller bry sig om riskerna utan enbart vill dra nytta av fördelarna som förekommer med IoT-enheter (Gilchrist, 2017; Wang et al., 2018). I studien styrktes detta då flera av testpersonerna värdesatte *funktionalitet* framför säkerhet när de valde att lämna en osäker enhet uppkopplad. För att stödja användares medvetenhet finns det därför ett behov av att informera användare om vilka *konsekvenser* det finns samt hur dessa kan påverka olika *funktioner* hos IoT-enheterna.

Utifrån diskussion framkom designförslaget: *Designa för att informera användare om potentiella konsekvenser av säkerhetsrisker och hur de påverkar funktionerna.*

5.4 Designelement 4: Social påverkan

Social norms kan användas för att influera personers besluttagande genom att informera om hur andra personer valt att agera (Thaler & Sunstein, 2008). För att designa för social norms kan text, statistik eller information som presenterar hur andra agerat användas för att påverka beslut (Hansen, 2016; Thaler & Sunstein, 2008). I prototypen utformades Designelement 4: Social påverkan genom att presentera att fyra av fem användare valt att koppla bort en osäker enhet från sina nätverk.

Testpersonerna uttryckte att informationen om att andra har agerat på ett visst vis var hjälpsamt och bidrog till en förståelse för att en enhet var utsatt. Två av testpersonerna som uttryckte att de hade mer teknisk erfarenhet jämfört med en vardaglig användare menade på att statistiken om hur andra agerat inte påverkade dem.

Mirsch et al. (2017) visar på att personer tenderar att följa den sociala normen istället för att bryta den. Detta framhävdes delvis i studien då vissa av testpersonerna valde att göra så som andra agerat medan andra ville ta reda på vad problemet var och agera därefter. Samtidigt uttryckte vissa av testpersonerna att statistiken kunde vara påträngande eller påtvingade.

Knuffar ska användas för få människor att utföra bättre beslut och inte begränsa deras fria vilja (Hansen, 2016; Mirsch et al., 2017; Thaler & Sunstein, 2008). Trots att en del av testpersonerna beskrev att statistiken kunde upplevas som påträngande begränsade det inte deras valalternativ. Digitala knuffar ska designas utan att begränsa eller förhindra valmöjligheter (Hansen, 2016; Mirsch et al., 2017; Thaler & Sunstein, 2008). Om statistiken som presenteras upplevs som påtvingande kan det förhindra eller begränsa användarens valalternativ, det är därför viktigt att designers tar detta i hänsyn vid design av digitala knuffar. Tidigare forskning menar att det är viktigt att knuffar implementeras med god avsikt för att göra det lättare för personer att göra bättre val (Acquisti et al., 2017; Hansen, 2016; Thaler & Sunstein, 2008). Statistiken som presenterades i designelementet påverkade testpersonerna och bidrog till att majoriteten uppmärksammade säkerhetsriskerna och hur allvarliga dessa var.

Utifrån diskussion framkom designförslaget: *Designa för att framhäva hur andra hanterat säkerhetsrisker genom statistik utan att vara för påträngande.*

Tabell 5 - Sammanställning av designförslag.

Designförslag	Beskrivning
Designa för att upplysa användaren om enhetens säkerhetsstatus genom färg och form.	Digitala knuffar bör designas med *visuell representation* som *färg* och *form* för att skapa en uppfattning kring enheters säkerhetsstatus. Dessa visuella representationer bör förklaras vid behov för användaren.
Designa för att göra det enkelt för användaren att utföra nödvändiga säkerhetsåtgärder och informera hur funktionerna påverkas.	Digitala knuffar bör designas med tydlig information och det ska vara enkelt för användare att ta säkra val. *Komplexitet* medför att användare inte agerar och utför därmed inte nödvändiga säkerhetsåtgärder. Därav bör det tydliggöras vad användare behöver göra för att få enheterna mer säkra och hur *funktionerna* kan påverkas.
Designa för att informera användare om potentiella konsekvenser av säkerhetsrisker och hur de påverkar funktionerna.	Digitala knuffar bör designas för att informera användare om eventuella *konsekvenser* av olika säkerhetsrisker. Användare vill veta

	detaljerat om *konsekvenserna* för att uppnå förståelse däremot bör det tydliggöras om och hur en enhets *funktioner* påverkas av säkerhetsrisker för att användare ska agera.
Designa för att framhäva hur andra hanterat säkerhetsrisker genom statistik utan att vara för påträngande.	Digitala knuffar bör designas genom att presentera *statistik* om hur andra hanterat säkerhetsrisker. Detta bidrar till en förståelse att användaren behöver se över säkerhetsriskerna. Viktigt att den presenterade informationen inte designas som påträngande eller påtvingade.

6 Slutsatser

I detta kapitel tas studiens syfte upp igen och en slutsats relaterat till resultatet visar på hur forskningsfrågan har besvarats. Avslutningsvis diskuteras det hur resultatet kan tillämpas i andra kontexter samt hur vidare forskning kan utföras.

Studien har ämnat att besvara frågeställningen: *Hur kan digitala knuffar designas för att stödja användares medvetenhet kring IoT-säkerhetsrisker i smarta hem?* Genom litteraturstudie identifierades att medvetenhet uppnås genom tre faser: uppfattning, förståelse och agera. Litteraturstudien låg även som grund till utformandet av prototypen där olika heuristiker samt designprinciper för digitala knuffar implementerades. För att undersöka hur medvetenhet kan stödjas genom digitala knuffar utfördes 10 utvärderingstester. Därefter analyserades datan som framkom från utvärderingarna för att sedan diskutera resultaten från analysen relaterat till resultatet i litteraturstudien. Ur diskussion framkom fyra designförslag:

- Designa för att upplysa användaren om enhetens säkerhetsstatus genom färg och form.
- Designa för att göra det enkelt för användaren att utföra nödvändiga säkerhetsåtgärder och informera hur funktionerna påverkas.
- Designa för att informera användare om potentiella konsekvenser av säkerhetsrisker och hur de påverkar funktionerna.

- Designa för att framhäva hur andra hanterat säkerhetsrisker genom statistik utan att vara för påträngande.

Designförslagen som tagits fram avses ligga till grund vid design av digitala knuffar för att stödja användarens medvetenhet kring IoT-säkerhetsrisker i smarta hem. Designförslagen kan vara användbara för att framhäva säkerhetsrisker som IoT-enheter har. I hänsyn till att IoT-tillverkare inte implementerar de nödvändiga säkerhetsriskerna hamnar ansvaret på användarna. Studien har framhävt att knuffarna kan användas trots att användare inte nödvändigtvis agerar. Istället kan de användas för att stödja medvetenhet kring IoT-säkerhetsrisker i smarta hem. Följaktligen kan knuffar användas för att göra användare mer kritiska avseende säkerhetsrisker hos IoT-enheter i sina privata hem. Detta kan i sin tur resultera i att IoT-tillverkare får påtryckning från konsumenter och implementerar nödvändiga säkerhetsfunktioner. Om användare inte blir informerade om de risker som finns leder det till att en stor mängd av de människor fortsätter att exponeras för risker. I takt med att användare fortsätter implementera IoT-enheter ovetande om säkerhetsrisker blir det allt mer viktigt att stödja deras medvetenhet.

Ur tidigare forskning kring knuffar har det framkommit att det är viktigt att det implementeras på ett icke-påträngande vis och inte leder till sämre val. För att undvika att knuffar används oetiskt är det viktigt att tydliggöra för olika val utan att begränsa användarnas valmöjlighet. En etisk aspekt som identifierades ur resultatet av utvärderingen var att statistik som visar på hur andra hanterat säkerhetsrisker kan upplevas som påtvingande och bör därför designas varsamt. Det är även viktigt att ta hänsyn till att digitala knuffar bör implementeras med god avsikt, det som innebär god avsikt för en part kan ha en annan innebörd för en andra part. Exempelvis kan en IoT-tillverkare ha andra uppfattningar om vad som är etiskt korrekt jämfört med en konsument. Det är viktigt att påpeka att designern har ett etiskt ansvar och bör överväga olika utkomster av dess design. De konsekvenser som en knuff kan bidra med bör alltid påverka personen på ett positivt vis, inte begränsa valmöjligheter och tillåta för att ta gynnsamma beslut.

I studien har det framställts att olika typer av digitala knuffar individuellt uppnår olika faser av medvetenhet. Därmed bör de olika digitala knuffarna designas i samband med varandra för att uppnå samtliga faser av medvetenhet hos användare. För att uppnå olika faser av medvetenhet identifierades olika teman som låg till grund till de fyra designförslagen. För att uppnå uppfattning framhävs att *visuell representation* kopplat till *form* och *färg* är viktigt. För att uppnå förståelse visar resultatet på att *konsekvenser* samt *statistik* är viktigt. Slutligen för att uppnå agera är det viktigt att *komplexitet* samt *funktionalitet* tas hänsyn till.

6.1 Vidare forskning

Studien har undersökt hur digitala knuffar kan designas för att stödja medvetenhet kring IoT-säkerhetsrisker i smarta hem och visar på hur olika digitala knuffar kan bidra till detta. För studien har enbart säkerhetsrisker inom IoT och smarta hem undersökts men vidare studier skulle kunna genomföras i andra områden för att testa vilka effekter förslagen uppnår.

I studien framställdes det att olika typer av digitala knuffar individuellt uppnår olika faser av medvetenhet. I studien har fyra heuristiker använts, framing, status quo bias, loss aversion och social norms. För att undersöka vidare skulle flera heuristiker vara lämpligt att studera för att få en djupare förståelse hur digitala knuffar kan designas och användas för att stödja medvetenhet.

7 Referenslista

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *IEEE security & privacy, 7*(6), 82-85. https://doi.org/10.1109/MSP.2009.163

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online, ACM Computing Surveys (Vol. 50, Issue 3, s. 1–41). *Association for Computing Machinery (ACM)*. https://doi.org/10.1145/3054926

Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes—Past, present, and future. IEEE transactions on systems, man, and cybernetics, part C (applications and reviews), 42(6), 1190-1203. https://doi.org/10.1109/TSMCC.2012.2189204

Almusaylim, Z. A., & Zaman, N. (2019). A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). *Wireless networks*, *25*(6), 3193-3204. https://doi.org/10.1007/s11276-018-1712-5

Ando, R., Shima, S., & Takemura, T. (2016). Analysis of privacy and security affecting the intention of use in personal data collection in an IoT environment. *IEICE TRANSACTIONS on Information and Systems, 99*(8), 1974-1981. https://doi.org/10.1587/transinf.2015INI0002

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless personal communications*, *58*(1), 49-69. https://doi.org/10.1007/s11277-011-0288-5

Bryman, A. (2018). *Samhällsvetenskapliga metoder* (Vol. 3). Liber

Chong, D., & Druckman, J. N. (2007). Framing theory. *Annu. Rev. Polit. Sci.*, *10*, 103-126. https://doi.org/10.1146/annurev.polisci.10.072805.103054

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Dennis, A. R., Yuan, L., Feng, X., Webb, E., & Hsieh, C. J. (2020). Digital nudging: Numeric and semantic priming in e-commerce. *Journal of management information systems*, *37*(1), 39-65. https://doi.org/10.1080/07421222.2019.1705505

Endsley, M. R. (1995). Measurement of situation awareness in dynamic systems. *Human factors*, *37*(1), 65-84. https://doi.org/10.1518/001872095779049499

Endsley, M. R. (2001). Designing for situation awareness in complex systems. *Proceedings of the Second International Workshop on symbiosis of humans, artifacts and environment* (pp. 1-14).

Endsley, M. R., & Garland, D. J. (Eds.). (2000). *Situation awareness analysis and measurement*. CRC Press.

Fahd Al-Mutawa, R., & Albouraey Eassa, F. (2020). A Smart Home System based on Internet of Things. *arXiv e-prints*, arXiv-2009. https://doi.org/10.48550/arXiv.2009.05328

Fejes, A., & Thornberg, R. (2019). *Handbok i kvalitativ analys.* Liber.

Gilchrist, A. (2017). *IoT Security Issues.* Berlin, Boston: De|G Press.

Google Play. (2022). *SmartThings*. Google play. https://play.google.com/store/apps/details?id=com.samsung.android.oneconnect&hl=sv&gl=US

Gross, T. (2013). Supporting effortless coordination: 25 years of awareness research. *Computer Supported Cooperative Work (CSCW)*, *22*(4), 425-474. https://doi.org/10.1007/s10606-013-9190-x

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71-80). https://doi.org/10.1145/1102199.1102214

Gutwin, C., & Greenberg, S. (2002). A descriptive framework of workspace awareness for real-time groupware. *Computer Supported Cooperative Work (CSCW), 11*(3), 411-446. https://doi.org/10.1023/A:1021271517844

Hansen, P. G. (2016). The definition of nudge and libertarian paternalism: Does the hand fit the glove?. *European Journal of Risk Regulation*, *7*(1), 155-174. https://doi.org/10.1017/S1867299X00005468

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

Kang, S., & Kim, S. (2017). How to obtain common criteria certification of smart TV for home IoT security and reliability. *Symmetry*, *9*(10), 233. https://doi.org/10.3390/sym9100233

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & security*, *28*(7), 509-520. https://doi.org/10.1016/j.cose.2009.04.006

Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management*, *62*, 102442. https://doi.org/10.1016/j.ijinfomgt.2021.102442

Lakhwani, K., Gianey, H. K., Wireko, J. K., & Hiran, K. K. (2020). *Internet of Things (IoT): Principles, Paradigms and Applications of IoT.* Bpb Publications.

Lee, H. (2020). Home IoT resistance: Extended privacy and vulnerability perspective. *Telematics and Informatics*, *49*, 101377. https://doi.org/10.1016/j.tele.2020.101377

Legg, P. A. (2016). Enhancing cyber situation awareness for Non-Expert Users using visual analytics. *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment* (CyberSA). 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA). IEEE. https://doi.org/10.1109/cybersa.2016.7503278

Lehner, M., Mont, O., & Heiskanen, E. (2016). Nudging – A promising tool for sustainable consumption behaviour? *Journal of Cleaner Production* (Vol. 134, s. 166–177). Elsevier BV. https://doi.org/10.1016/j.jclepro.2015.11.086

Lim, Y.-K., Stolterman, E., & Tenenberg, J. (2008). The anatomy of prototypes: Prototypes as filters, prototypes as manifestations of design ideas. *ACM Transactions on Computer-*

Human Interaction, 15(2), 1–27. https://doi.org/10.1145/1375761.1375762

McDermott, C., Isaacs, J., & Petrovski, A. (2019). Evaluating Awareness and Perception of Botnet Activity within Consumer Internet-of-Things (IoT) Networks. *Informatics 6*(1, s. 8). MDPI AG. https://doi.org/10.3390/informatics6010008

Mirsch, T., Lehrer, C., & Jung, R. (2017). Digital nudging: Altering user behavior in digital environments. *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, 634-648.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys & Tutorials 21*(Issue 3, s. 2702–2733). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/comst.2019.2910750

Niemantsverdriet, K., Essen, H. V., Pakanen, M., & Eggen, B. (2019). Designing for Awareness in Interactions with Shared Systems. *ACM Transactions on Computer-Human Interaction 26* (Issue 6, s. 1–41).

Association for Computing Machinery (ACM). https://doi.org/10.1145/3338845

Preece, J., Rogers, Y., & Sharp, H. (2019). *Interaction design: Beyond human-computer interaction.* New York, NY: J. Wiley & Sons.

Rice, M. D., & Bogdanov, E. (2018). Privacy in Doubt: An Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices. *Canadian Journal of Administrative Sciences / Revue Canadienne des Sciences de l'Administration 36*(Issue 2, s. 163–176). Wiley. https://doi.org/10.1002/cjas.1494

Schneider, C., Weinmann, M., & vom Brocke, J. (2018). Digital nudging. *Communications of the ACM* (Vol. 61, Issue 7, s. 67–73). Association for Computing Machinery (ACM). https://doi.org/10.1145/3213765

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015, October). Network-level security and privacy control for smart-home IoT devices. In *2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 163-167). IEEE. https://doi.org/10.1109/WiMOB.2015.7347956

Streiff, J., Das, S., & Cannon, J. (2019). Overpowered and Underprotected Toys Empowering Parents with Tools to Protect Their Children. *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC*). IEEE. https://doi.org/10.1109/cic48465.2019.00045

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness.* Yale University Press.

Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2010). Choice Architecture. *SSRN Electronic Journal.*

Tracy, S. J. (2010). Qualitative Quality: Eight "Big-Tent" Criteria for Excellent Qualitative Research. *Qualitative Inquiry 16*(Issue 10, s. 837–851). SAGE Publications. https://doi.org/10.1177/1077800410383121

Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A. (2015). Nudging towards security. *Proceedings of the 2015 British HCI Conference.* British HCI 2015: 2015 British Human Computer Interaction Conference. ACM. https://doi.org/10.1145/2783446.2783588

Wang, X., McGill, T. J., & Klobas, J. E. (2018). I Want It Anyway: Consumer Perceptions of Smart Home Devices. *Journal of Computer Information Systems 60*(Issue 5, s. 437–447). Informa UK Limited. https://doi.org/10.1080/08874417.2018.1528486

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly, 26*(2), xiii–xxiii. http://www.jstor.org/stable/4132319

Weinmann, M., Schneider, C., & Brocke, J. vom. (2016). Digital Nudging. Business & Information Systems Engineering *58*(Issue 6, s. 433–436). *Springer Science and Business Media LLC*. https://doi.org/10.1007/s12599-016-0453-1

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal, 4*(5), 1250-1258. https://doi.org/10.1109/JIOT.2017.2694844

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal 6*(Issue 2, s. 1606–1616). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/jiot.2018.2847733

Zimmerman, J., Forlizzi, J. (2014). Research Through Design in HCI. Olson, J., Kellogg, W. (eds) *Ways of Knowing in HCI.* Springer, New York, NY. https://doi.org/10.1007/978-1-4939-0378-8_8

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems* (Vol. 62, Issue 1, s. 82–97). Informa UK Limited. https://doi.org/10.1080/08874417.2020.1712269

8 Bilagor

Bilaga 1 - Talarmanus

Studiens syfte är att studera säkerhetsriskerna kring IoT-enheter i smarta hem och medvetenheten kring dessa. Med IoT-enheter menar vi Internet of Things, alltså saker som är uppkopplade till internet. Dessa kan vara en robotdammsugare, Google home, smart-TV eller liknande. Inga personliga uppgifter kommer användas till studien. Datan, dina upplevelser kring prototyptestet, kommer enbart användas till denna studie och med största sekretess. Om du upplever obehag eller stress eller av någon anledning och inte längre vill delta i studien är helt okej att avbryta studien utan att ange anledning.

Vet du vad IoT är?

Förstår du studiens syfte och samtycker till att delta i undersökningen?

Är det okej att vi spelar in?

Bilaga 2 - Scenario och uppgifter

Avsikten med utvärderingen är att se hur ett verktyg kan öka medvetenhet om säkerhetsrisker med IoT-enheter i det smarta hemmet. Med IoT-enheter menar vi Internet of Things, alltså saker som är uppkopplade till internet. Dessa kan vara en robotdammsugare, uppkopplad ringklocka, Google home, smart TV eller liknande. Prototypen är i ett tidigt stadie och vissa funktioner och knappar fungerar inte. För utvärderingen kommer du successivt få uppgifter att utföra. Det hjälper oss väldigt mycket om du berättar hur du tänker när du utför uppgifterna. Samtidigt kan det ske att vi ställer frågor under utvärderingen. Du får också ställa frågor till oss men det är inte säkert vi alltid kan svara för att det kan påverka resultatet.

I detta scenario har du laddat ner en app som tillåter dig att se dina IoT-enheter i hemmet och se över säkerheten av dessa.

Uppgift 1: Se enheternas säkerhet i hemmet.

Uppgift 2: Se över vilka säkerhetsrisker Samsung TV är utsatt för.
Uppgift 3: Gör din enhet mer säker om det går.

Uppgift 4: Se över vilka säkerhetsrisker Philips Hue Light är utsatt för.
Uppgift 5: Gör din enhet mer säker om det går.

Uppgift 6: Se över vilka säkerhetsrisker FIBARO Wallplug audio är utsatt för.
Uppgift 7: Gör din enhet mer säker om det går.

Uppgift 8: Se över vilka säkerhetsrisker FIBARO Light switch är utsatt för.
Uppgift 9: Gör din enhet mer säker om det går.

Bilaga 3 - Intervjuguide

Före prototyptest
Standardfrågor
Kan du berätta om din bakgrund relaterat till IoT?
Hur gammal är du?
Hur ser du på säkerheten när du är inne på internet?
Hur många IoT-enheter har du uppkopplade i ditt hem ungefär?
Hur ofta använder du IoT-enheter / enheten?
Hur ser du på säkerheten för IoT?

Efter prototyptest
Öppna frågor
Vad tror du prototypens syfte var?
Hur upplevde du prototypen?
    Vad fick dig att känna dig så?
Vad det något i prototypen som du uppmärksammade extra mycket?
    Varför uppmärksammade du det extra mycket?
Hur är ditt synsätt på säkerhet inom IoT nu?
Hade du använt ett sådant verktyg?
    Varför / Varför inte?

Designelement 1: Säkerhetsstatus
Vad tänkte du om smileysarna?
Vad tänkte du om färgerna? (I smileysarna)
Tyckte du de var nödvändiga för att förstå enhetens status?
    Varför / Varför inte?
Hade du förstått med färgerna fast utan smileysarna?
    Varför / Varför inte?
Hade färgerna påverkat dig?
    Varför / Varför inte?
Hade du förstått med smileysarna fast utan färgerna?
    Varför / Varför inte?
Hade smileysarna påverkat dig?
    Varför / Varför inte?

Designelement 2: Automatiska uppdateringar
Vad tänkte du efter du valt Philips Hue lampan inför valet vid att sätta på automatiska uppdateringar?
Vad tänkte du om att alternativet var förvalt?
    Varför tänkte du så?
Förstod du att du kunde ändra val?
Påverkade det ditt beslut att det var förvalt?
    Varför / Varför inte?

Designelement 3: Varningsmeddelande
Vad tänkte du om texten som visas för konsekvenserna om du inte uppdaterar Samsung TV?
Vad tänkte du om informationen som gavs för att uppdatera TV?
Hade du uppdaterat TVn i verkligheten?
    Varför / Varför inte?
Vad tänkte du om popupen som kom för FIBARO wallplug audio/Samsung TV?
Påverkade det ditt beslut?
Vad tänkte du om texten?
Hade du stängt av enheten i verkligheten?
    Varför / Varför inte?

Designelement 4: Social påverkan
Vad tänkte du när du såg att 4 av 5 kopplat ifrån sin enhet?
Kände du att det påverkade ditt beslut?
    Varför / Varför inte?
Hade du tänkt annorlunda om texten inte var med?
    Varför / Varför inte?
Hade du kopplat ifrån enheten i verkligheten?
    Varför / Varför inte?

Bilaga 4 - Prototyp

https://www.figma.com/proto/gX0Iqqf4nnCG5aevPRAgDQ/Kandidatuppsats?node-id=41%3A124&scaling=scale-down&page-id=0%3A1&starting-point-node-id=41%3A124