

Allmänna kunskap kring cybersäkerhet bland pensionärer

Kunskap kring datasäkerhet för människor från ålder 65 och uppåt

General knowledge about cybersecurity among senior citizens

Knowledge about data security for people aged 65 and over

Författare: Ali Adrian Nasrat, Porsche Thichan, Vilmer Skoglund.

Nivå: Grundnivå

Kursnamn: Forskningsmetodik

Kurskod: GIK34Y

Högskolepoäng: 3

Handledare: William Wei Song

Institution: Institutionen för Informatik och Teknik

Examinator: Madelen Lagin

Examinationsdatum: 2024-05-27

Vid Högskolan Dalarna finns möjlighet att publicera examensarbetet i fulltext i DiVA. Publiceringen sker Open Access, vilket innebär att arbetet blir fritt tillgängligt att läsa och ladda ned på nätet. Därmed ökar spridningen och synligheten av examensarbetet.

Open Access är på väg att bli norm för att sprida vetenskaplig information på nätet. Högskolan Dalarna rekommenderar såväl forskare som studenter att publicera sina arbeten Open Access.

Jag/vi medger publicering i fulltext (öppet tillgänglig på nätet, Open Access):

Ja ☐

Nej ☒

Innehållsförteckning

1. INLEDNING
 - 1.1. BAKGRUND
 - 1.2. PROBLEMFORMULERING
 - 1.3. SYFTE OCH FORSKNINGSFRÅGOR
 2. TEORI
 - 2.1. CYBERSÄKERHET
 - 2.1.1. CYBERATTACK
 - 2.1.2. SOCIAL MANIPULATION
 - 2.2. CYBERSÄKERHET OCH PENSIONÄRER
 3. METOD
 - 3.1. SYSTEMATISK LITTERATURSÖKNING
 - 3.2. METODSTRATEGI
 - 3.3. DATAINSAMLINGSVERKTYG
 - 3.3.1. ENKÄT
 - 3.3.2. INTERVJU
 - 3.4. URVALSPROCESS
 - 3.4.1. POPULATION
 - 3.4.2. URVALSRAM
 - 3.5. DATAINSAMLING
 - 3.5.1. ENKÄT
 - 3.5.2. INTERVJU
 - 3.6. DATABEARBETNING OCH ANALYS
 - 3.6.1. DATABEARBETNING
 - 3.6.2. ANALYS
 - 3.7. RELIABILITET, VALIDITET OCH FORSKNINGSETIK
 - 3.7.1. RELIABILITET OCH VALIDITET
 - 3.7.2. FORSKNINGSETIK
 4. EMPERI
 5. ANALYS
 6. DISKUSSION
 7. SLUTSATS
 - 7.1. SLUTSATSER
 - 7.2. METODDISKUSSION
 - 7.3. REFLEKTION ÖVER DEN EGNA PROCESSEN
- REFERENSER
- BILAGA 1: MISSIVBREV TILL ENKÄT
- BILAGA 2: ENKÄTFORMULÄR
- BILAGA 3: MISSIVBREV TILL INTERVJU
- BILAGA 4: INTERVJUFORMULÄR
- BILAGA 5: TRANSKRIBERING AV INTERVJU(ER)

Allmänna kunskap kring cybersäkerhet bland pensionärer

Sammanfattning

Rapporten undersöker pensionärers behov av utbildning kring cybersäkerhet samt anledning till att pensionärer är främsta målgruppen för cyberhot. I dagens samhälle där användning och utvecklingen av digitala tjänster har ökat exponentiellt har även cyberhot blivit alltmer vanligare. Pensionärer som saknar kunskaper kring digitala tjänster har svårt att hänga med den snabba utvecklingen och detta skapar en stor möjlighet för bedragare att utnyttja denna brist på kunskapen för att begå cyberbrott.

Undersökningen sker med litteratursökning, en enkät, och två intervjuer. Resultatet från enkäten visar att en stor mängd av pensionärerna som svarade på enkäten känner sig osäkra online, där anledningen visas bero på brist av kunskap om cybersäkerhet, där yngre åldersgrupper har mer koll på vad för bedrägeri som finns. Intervjuerna gjordes på en 65 årig man och en 23 årig man för att kunna jämföra deras upplevelser med cybersäkerhet online. Den 65 årige mannen visades föredra digitala tjänster över icke-digitala, men var försiktig att ej gå in på okända sidor. Han hade aldrig blivit utsatt för någon form av cyberattack. Den 23 årige mannen hade generellt ej någon preferens mellan digitala och icke-digitala tjänster, men visades ha en grundläggande kunskap om cybersäkerhet och de hot som händer. Han hade haft kompisar som blivit utsatta för stölder av konton och liknande, men hade ej blivit offer i det själv.

Sammanfattningsvis kom studien fram till att bristen på kunskap och information om cybersäkerhet hos pensionärer för fram en rädsla och får dem att ej sträva för långt utanför vad de är bekväma med online. Det identifierades att det behövs någon typ av utbildning eller tjänst som kan hjälpa pensionärer att säkert existera online.

Nyckelord

cybersäkerhet, pensionärer, online, cyberattack,

Abstract

This study investigates the need for cybersecurity education among senior citizens and the reasons why they are the primary target for cyber threats. Today, where the use and development of digital services have increased exponentially, cyber threats have also become more common. Senior citizens, who lack knowledge about digital services, find it challenging to keep up with the rapid development of technology, creating significant opportunities for fraudsters to exploit this lack of knowledge to commit cybercrimes.

The study's investigation was conducted through a literature review, a survey, and two interviews. The results from the survey indicate that a significant number of senior citizens who responded feel insecure online, primarily due to a lack of knowledge around cybersecurity, whereas younger age groups are more aware of various types of online fraud. The interviews were conducted with a 65-year-old man and a 23-year-old man to compare their experiences with online cybersecurity. The 65-year-old man preferred digital services over non-digital ones but was cautious about visiting unfamiliar websites, and thus had never been the victim of any cyberattacks. The 23-year-old man had no general preference between digital and non-digital services but demonstrated a basic understanding of cybersecurity and current online threats. He'd had friends who had experienced account theft and similar issues but had not been a victim of it himself.

The study concluded that the lack of knowledge and information about cybersecurity among senior citizens foster fear for digital activity and discourages them from exploring beyond their comfort zone online. It was identified that there is a need for some form of education or service to help senior citizens navigate the online world safely.

Keywords

cybersecurity, senior citizens, online, cyberattack

1. Inledning

1.1. Bakgrund

I dagens samhälle har användningen av internet och allt digitalt ökat exponentiellt. Samtidigt har behovet av att förstå och förhindra potentiella hot online blivit alltmer viktigare, speciellt för pensionärer. Deras begränsade digitala erfarenheter gör det enklare för dem att utsättas för olika sorters av potentiella hot som till exempel 'phishing' och 'pharming', vilket i sin tur kan hjälpa och vara ett underlag för identitets stöld (Brody R. G, 2007). Många pensionärer från cirka 65 år gamla och uppåt saknar just de förkunskaper för att åtgärda dessa hot eller förutse dessa potentiella risker (Grimes G. A, 2010). Samtidigt är pensionärer den främsta målgruppen för dessa hot på grund av faktorer som kognitiv funktionsnedsättning, bristande ekonomisk kunskap, oförmåga att hantera ekonomi, sensorisk förlust och känslomässig sårbarhet (Appelt L. C, 2016).

1.2. Problemformulering

Trots att det finns tillgång till flera studier kring cybersäkerhet så har flera av dessa studier åldrats och det behövs en förnyelse. Nu när medellivslängden har ökat och kan fortsätta att öka betyder det att fler pensionärer kommer att utsättas för användning av internet och digitala tjänster. Det finns studier som visar på dessa risker samt behovet att skydda denna studies målgrupp från riskerna, men det kvarstår frågor kring hur de befintliga åtgärder och resurser kan hjälpa den sårbara gruppen om dessa åtgärder och resurser är tillräckliga. Dessutom är det brist på förståelse för faktorerna som gör pensionärer till attraktiva mål för cyberkriminalitet. Därför är det viktigt att problematisera och undersöka om det finns behov av samhället att med dess resurser åtgärda utbildningar för att bättre skydda den sårbara befolkningsgruppen från online/digitala hot och risker samt stärka deras digitala förmågor för att ge dem en bättre online miljö.

1.3. Syfte och forskningsfrågor

Syftet med denna studie är att problematisera och undersöka om det finns behov av att bättre skydda äldre och pensionärer från digitala hot och risker med dess resurser som finns dessutom förbättra deras digitala förmågor att identifiera samt undvika de befintliga hot och risker. Denna forskning syftar att bidra till en uppdaterad och mer omfattande förståelse för äldres digitala säkerhet genom att analysera befintliga studier och identifiera de kunskapsluckor samt brister i

förståelsen för faktorer som gör pensionärer till attraktiva mål för cyberkriminalitet. Forskningsfrågorna är följande:

Vad är den genomsnittliga kunskapsnivån för pensionärer kring cybersäkerhet?

Finns det behov av utbildning för pensionärer och äldre kring cybersäkerhet?

2. Teori

För att kunna forska om cybersäkerhet samt cyberhot krävs en förståelse för de nyckelbegreppen och teorier som är relevanta för ämnet. Detta fungerar som en grund och underlag för analys och diskussion som uppkommer senare i studien. Genom att dra nytta av befintlig kunskap och fördjupa förståelsen kan forskning leda till framsteg och skapa ny insikt inom det aktuella området.

2.1. Cybersäkerhet

Cybersäkerhet innebär skyddet av både digital information och den infrastruktur som är nödvändig för att säkerställa att den digitala informationen fungerar korrekt och är tillgänglig. Det inkluderar att säkra data, programvara, informationssystem, hårdvara och nätverk från olika former av hot och attacker. För att få en hög säkerhetsnivå är det avgörande att även hanteringen av information och data sker på ett säkert sätt för att förhindra oavsiktlig förstörelse (Lindholm, C).

Termen cybersäkerhet används i olika sammanhang, det kan vara från affärsapplikationsdomäner till mobile computing. Cybersäkerhet kan grupperas i olika kategorier som till exempel applikationssäkerhet, datorsäkerhet, datasäkerhet, informationssäkerhet, nätverkssäkerhet, driftsäkerhet, katastrofåterställning, affärskontinuitet, osv. Därför är cybersäkerhet en praxis för att skydda känsliga data från obehörig åtkomst (Möller, P.F., Dietmar, 2023).

2.1.1. Cyberattack

Cyberattack innefattar attacker mot digitala tillgångar. Syftet med detta är vanligen att komma åt, ändra eller förstöra känslig information. Olika typer av attack som kan ske är till exempel cyberbrott, cyberkrigsföring, och cyberterrorism. I denna studie kommer fokus läggas på cyberbrott vilket innebär att enstaka individer eller grupper angriper ett system, där målet oftast är för ekonomisk vinning (Lindholm, C).

2.1.2. Social manipulation

Social manipulation innebär att en användare luras till att avslöja information som påverkar IT-säkerheten, till exempel ett viktigt lösenord. Detta kan ske genom *spoofing* vilket innebär att man använder en förfalskad avsändaradress i e-postmeddelanden eller spam, vilket i sin tur innebär ett massutskick av meddelande på internet som mottagaren skulle avstått att erhålla vid fritt val, till exempel reklam (Nationalencyklopedin [NE], u.å.). E-postadressen blir då förfalskad så att den ser ut som att den kommer från en trovärdig avsändare. Detta förfarande används vid *phishing* vilket är en välkänd typ av attack där målet är att stjäla känslig information så som användarnamn, lösenord, och kreditkortsnummer (Lindholm, C).

2.2. Cybersäkerhet och pensionärer

Med den snabba utvecklingen av internet och digitala tjänster tillkommer många förmåner i vardag för folk, dock så har pensionärer svårare att vänja sig vid och dra nytta av dessa digitala tjänster på grund av skäl som ålder, kognitiva färdigheter och utbildning.

Pensionärer har blivit en grupp som är överrepresenterad när det kommer till digitalt utanförskap, där huvudanledningen är rädslan för att bli offer för cyberattack genom att använda digitala tjänster och teknik. Rädslan grundar sig sannolikt i en brist på färdigheter och kunskap som behövs för att dra full nytta av allt som digitala tjänster och internet har att erbjuda. Dessutom är den snabba utvecklingen av digitaliseringen en annan faktor; den kräver att användarna hela tiden anpassar sig till nya tekniker för att undvika att bli överlämnade åt sitt öde. Detta utgör en betydande utmaning för äldre personer (Holgersson et al., 2021; Holgersson & Söderström, 2019).

3. Metod

Denna studie strävar efter att undersöka och problematisera hur samhället kan förbättra skyddet för äldre och pensionärer mot digitala hot och risker genom att utnyttja befintliga resurser samt stärka deras digitala kompetens för att bättre kunna identifiera och undvika dessa hot. Syftet är att bidra till en mer uppdaterad och omfattande förståelse för äldres digitala säkerhet och för att uppnå detta kommer metoden som genomförs vara systematisk litteratursökning, och en

kombination av kvantitativa och kvalitativa analys, som kallas för mixed-methods. Den kvantitativa analysen kommer att fokusera på att sammanställa och analysera svar från enkät för att identifiera mönster och trender i hur människor i olika ålder upplever säkerheten med att använda internet och digitala tjänster. Den kvantitativa analysen kommer att utforska detaljerat teman och mönster genom analys av en semistrukturerad intervju med deltagare, vilket ger en mer detaljerad förståelse för deras upplevelser och perspektiv på ämnet. Genom dessa metoder strävar studien efter en holistisk och nyanserad förståelse av äldres digitala säkerhet och sårbarhet.

3.1. Systematisk litteratursökning

För att hitta forskningar och texter som är relevanta till denna studies ämne så har sökmotorerna som använts inkluderat Högskolan Dalarnas databasbibliotek, Summon, samt sökmotorn Google Scholar. Med dessa två bibliotek kan man söka med söksträngar som inkluderar nyckelord som associerar med studiens ämne. I tabellen nedan kan man observera olika steg av sökningen med nyckelorden som använts, logiken bakom valet av söksträng, och resultatet av sökningen.

Sökning	Söksträng	Logik Bakom	Summon	Google Scholar	Är resultatet rimlig?
1	“cybersecurity”	Vårt huvudligaämne handlar främst om cybersäkerhet.	89,234	738,000	Ja, för att söksträngen endast ett nyckelord som är ganska vanlig
2	“cybersecurity” AND “pensioner”	Vi vill ha information om säkerheten kring vår målgrupp.	6	234	Nej, vi behöver breda ut resultatet mer
3	“cybersecurity” AND (“pensioner” OR “senior citizen”)	För att få fler resultat behövs även bredare söksträng, vi använder oss då utav ord som betydelsen liknar varandra.	25	565	Ja, resultatet är rimligt

Sökningen sker på engelska så att sökträffen ska vara så bred som möjligt. Vid första steget består söksträngen endast utav “cybersecurity” som en grund för att bygga vidare på. Resultatet var omfattande, vilket förväntades. För att förfinasökningen inkluderades målgruppen i nästa steg, med användning av booleska operatorn "AND", vilket ledde till mer relevanta resultat. Ordet “pensioner” valdes vid denna steg och resultatet blev mer relevant men samtidigt ansågs ändå

vara för begränsat. Till slut för att öka mängden resultat används booleska operatoren OR inom parentes mellan nyckelordet “pensioner” och “senior citizen”. Det resulterande urvalet var betydande och många av resultaten ansågs vara relevanta och användbara.

3.2. Metodstrategi

Denna studie använder både kvantitativ och kvalitativ forskning. Dessa metoder valdes på grund av deras kompletterande natur, vilket ger studien en mer nyanserad förståelse av studiens ämne. Den kvantitativa data kommer att bidra till majoriteten av studiens insamlade data, där dessa data samlas in genom en enkät. Kvalitativa data kommer att hämtas från studiens intervjuer där dess data beskriver respondenternas personliga erfarenheter, åsikter och uppfattningar i mer detalj. Genom att kombinera dessa två datainsamlingsmetoder kan breda trender och mönster mätas och analyseras samtidigt som de underliggande orsakerna och kontexter bakom dem kan förstås bättre. Detta säkerställer att studien täcker både bredd och djup, vilket ger en rikare och mer heltäckande bild av forskningsämnet.

3.3. Datainsamlingsverktyg

Denna studies datainsamling använder en enkät för den kvantitativa data, och två intervjuer för kvalitativa data. Enkäten publiceras online för att få en bred kvantitativ data om respondenternas erfarenhet och åsikter kring cybersäkerhet och cyberhot. De två intervjuerna kommer att samla in djupa kvalitativa data kring studiens ämne.

3.3.1. Enkät

Microsoft Forms är den tjänsten som används för denna studies enkät, då den är lättförståelig för respondenter när de svarar på den och den är lätt att arbeta med. Enkäten kommer även att delas ut i person på papper och sedan matas in i enkäten på Microsoft Forms.

3.3.2. Intervju

De två intervjuerna sker i person. Där kommer de inspelas via mobil för att sedan transkriberas med hjälp Microsoft Words transkriberings funktion. Då en automatisk transkribering inte är perfekt behöver den också granskas manuellt för att fixa feltranskriberingar.

3.4. Urvalsprocess

Även fast denna studie syftar på datasäkerhet hos personer 65 år och äldre var aspekten att ha ett större urval av grupper viktigt för att kunna få en bredare jämförelse.

3.4.1. Population

Som tidigare nämnt är det viktigt att ha fler än bara personer 65 år och äldre för att kunna få en bra jämförelse och se vilka skillnader och liknelser som finns i deras svar.

3.4.2. Urvalsram

Studiens enkät sprids till personer i alla åldrar med undantag att man ska vara över 18 år gammal. Detta är så att skillnaden mellan olika åldrar kan jämföras och analyseras. Den geografiska spridningen av enkäten sker främst inom Rättvik, Orsa, och Borlänge, då författarna delar ut enkät fysiskt till dessa områden. Enkät svar som sker online kan ej spåras geografiskt.

Utmaningen med studiens målgrupp, vilket i studiens fall är pensionärer, var att enkäten nådde ut till endast få tal. Genom att dela ut fysisk enkät offentligt kan enkäten lättare nå fram till målgruppen.

Två personer har kontaktats för att genomföra intervjun. Av dessa två är en 23 år gammal och en 65 år gammal. Dessa respondenter har olika bakgrund samt erfarenheter med användning av internet och digitala tjänster vilket ger författarna bredare perspektiv på ämnet om cybersäkerhet.

3.5. Datainsamling

Enkäten lämnades ut först. Detta valdes till studien då den kvantitativa data kan analyseras för att sedan anpassa intervjufrågorna till den kvalitativa data som blir insamlad genom senare intervju. Dock inkom ej alla svar från enkäten inom tidsramen, så alla svar från enkäten kunde ej bli besvarade i tid för att analyseras inför intervjun. Därför anpassades intervjufrågorna till de resultat som kom in tidigt.

3.5.1. Enkät

Enkäten använder sig av 2 kategoriseringsfrågor, 10 frågor med förbestämda svar (exempelvis: välj från 1–5), och en följdfråga där respondent kan skriva eget svar beroende på föregående frågans svar.

De två kategoriseringsfrågorna bestod av fråga om kön och ålder. Könnsfrågan kan vara viktig för att visa om det finns några mönster runt detta, och frågan om ålder, som förklarad tidigare i texten, är viktigt för att se samma sak då enkäten bör ha ett brett urval.

Enkäten distribueras främst online via sociala medier och e-mail. Den distribuerades även i person där enkäten gavs ut i pappersform.

Alla respondenter och deras svar är totalt anonyma förutom de två kategorifrågorna som frågar efter kön och ålder, men respondenterna efterfrågas ej namn eller någon annan identifierande fråga.

3.5.2. Intervju

Intervjun sker semi strukturerat med en bakgrundsfråga och sju huvudfrågor som kan senare utvecklas. Semistrukturerade intervjuer valdes eftersom de ger respondenterna möjlighet att utveckla sina svar, vilket kan ge mer djupgående information. Det kan även ge respondenterna en tryggare miljö där de känner sig bekväma att dela sina åsikter och erfarenheter utan rädsla för att bli dömda eller att deras information ska missbrukas. Frågor som ställs under intervjun är utformade för att assistera författarna analys kring ämnet för studien.

3.6. Databearbetning och analys

3.6.1. Databearbetning

Studien använder sig av enkäter från Microsoft Forms, som sedan kommer att läggas in och bearbetas i Microsoft Excel, där Pivot Table används för att summera all data från enkätsvaren.

3.6.2. Analys

Genom att använda Pivot Table för alla enkätsvar kan vi simpelt analysera, jämföra och hitta samband mellan olika svar och olika frågor.

Självaste intervjun analyseras genom att gå igenom alla svar och identifiera kopplingar mellan dem. Studien jämför även svaren mellan alla intervjuer för att se om det finns kopplingar och sådant.

3.7. Reliabilitet, validitet och forskningsetik

3.7.1. Reliabilitet och validitet

Studien kommer att använda triangulering vilket innebär undersökning av ett visst studieobjekt genom användning av två olika metoder. I studiens fall använder den sig utav Datatriangulering, och det innebär att flera olika datakällor används till en undersökning (Björklund & Paulsson, 2012). I studiens fall använder vi enkäter och en semistrukturerad intervju vilket ökar validiteten samt reliabiliteten i undersökningen.

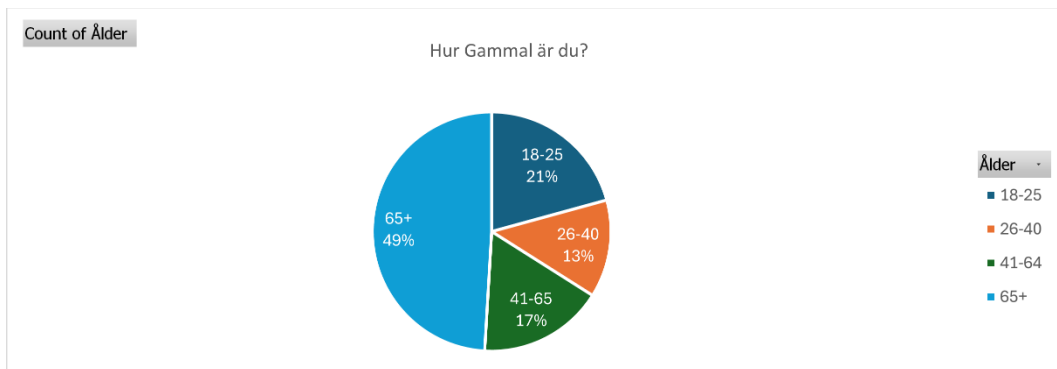
3.7.2. Forskningsetik

Inför enkäten och intervjun ställs frågor till respondenter om deras samtycke där respondenten informeras om deras konfidentialitet samt anonymitet. Genom att informera respondenten om studiens syfte, vad frågorna kommer handla om, samt vad deltagandet innebär för dem, kan vi säkerställa att deltagarnas integritet skyddas samt att deras medverkan är informerad och frivillig.

4. Empiri

Enkäten som delades ut fick tillbaka 53 svar varav 49% är över 65 år gamla och 55% är män. Enkäten visar att de flesta respondenter använder internet och digitala tjänster varje dag. Sedan visas variation av svar kring hur säkra de känner sig med att hantera personlig information online, där svaret var mer utspritt. Majoriteten delar inte ut deras bankinformation utan att vara säkra på att det är en legitim källa. Sedan kan man observera att 64% svarade att de har fallit offer för phishing-attack online och sedan 60% svarade att de kände till olika metoder som bedragare använder online. 74% av respondenterna har ej fått en utbildning eller information om cybersäkerhet och hur man skyddar sig mot en cyberattack. Men samtidigt anser 64% att det finns ej tillräckligt med stöd och tillgänglig utbildning för de som behöver det. De flesta anser att de har låg kunskap kring cybersäkerhet men ändå föredrar majoriteten av respondenterna att använda digitala tjänster. Dock beskrivs anledning i sista frågan för de som har valt att de föredrar icke-digitala tjänster. Där skrivs det kommentarer såsom "För krångligt", "Osäkerhet", "Jag litar inte på dator sidor". Nedan visas ett diagram för alla frågor från enkäten med undantag till frågan om samtycke:

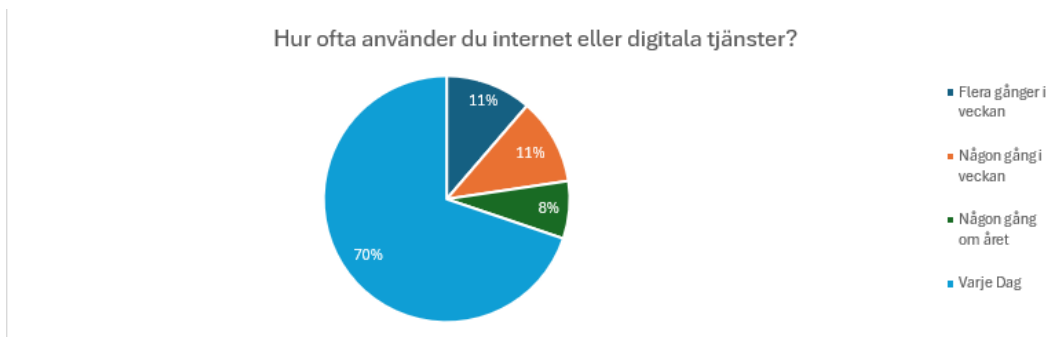
Allmänna kunskap kring cybersäkerhet bland pensionärer



Figur 1, åldersfördelning.

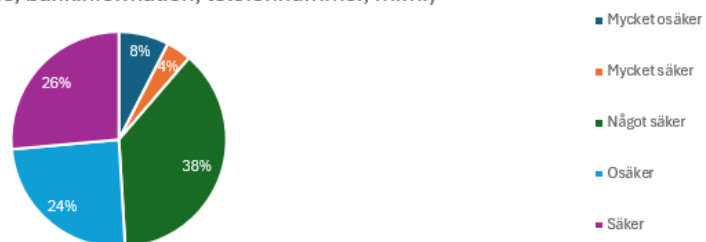


Figur 2, könsidentitet.



Figur 3, användning av internet eller digitala tjänster.

Hur säker känner du dig när det gäller att hantera personlig information online?
(Adress, bankinformation, telefonnummer, m.m.)



Figur 4, säkerhet kring hantering av personlig information online.

Har du någonsin delat dina bankuppgifter eller personlig information med någon online utan att först verifiera att det var en legitim källa?



Figur 5, frågan om delning av bankuppgifter eller personlig information.

Har du någonsin klickat på en länk eller en annons som du sett online?



Figur 6, frågan om de har klickar på annons eller länkar online.

Har du någonsin fallit offer för en phishing-attack online??



Figur 7, offer för online phishing-attack.

Känner du till vanliga metoder som används av bedragare för att lura människor online? (Exempel: phishing, skräppost, falska webbplatser)



Figur 8, kännedom om vanliga metoder för att lura människor online.

Har du någonsin fått utbildning eller information om cybersäkerhet och hur man skyddar sig mot cyberattacker?



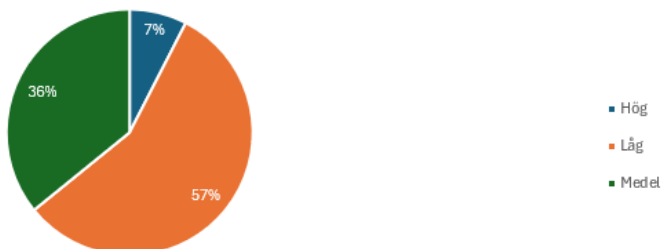
Figur 9, frågan om utbildning kring cybersäkerhet.

Tycker du att det finns tillräckligt med stöd och tillgänglig utbildning om cybersäkerhet för dem som behöver det?



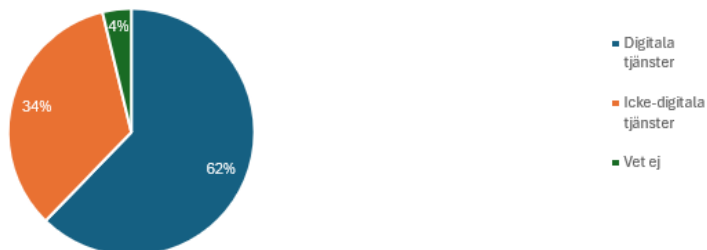
Figur 10, stöd och tillgänglig utbildning.

Hur skulle du beskriva din kunskap om cybersäkerhet?



Figur 11, frågan kring kunskap om cybersäkerhet.

Föredrar du generellt att använda digitala tjänster eller icke-digitala tjänster?



Figur 12, digitala tjänster och icke-digitala tjänster.

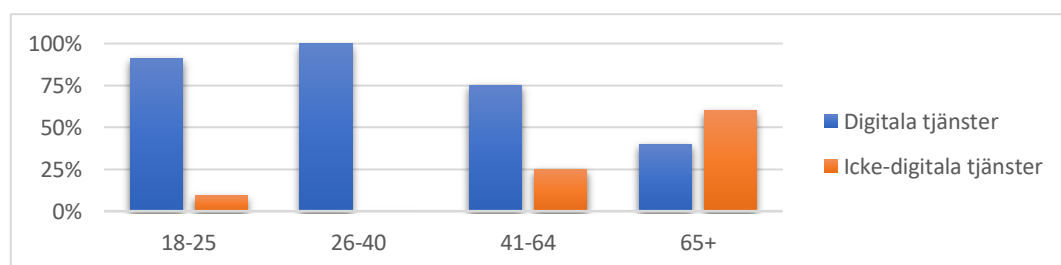
Resultaten från intervjun visar att respondent 1, en 65-årig man, använder internet dagligen för Facebook och nyheter. Han är självlärd inom internetsäkerhet och undviker annonser på webbsidor. Han använder samma lösenord för flera tjänster, känner till och använder tvåfaktorsautentisering, och har antivirusprogram.

Respondent 1 föredrar digitala tjänster för nyheter och handel, men är försiktig med okända sidor. Han anser att det bör finnas enklare och tydligare information om internetsäkerhet för äldre.

Respondent 2, en 23-årig man, använder internet flera gånger dagligen och har inte fått utbildning i internetsäkerhet. Han är försiktig med länkar från okända källor och använder antivirusprogram och tvåfaktorsautentisering, även om han ibland undviker det. Han har få lösenordsvariationer och föredrar fysiska butiker för kläder och tidningar för nyheter men handlar även online produkter han använd innan, och använder både digitala och icke-digitala tjänster lika mycket. Respondent 2 anser att fler i hans generation behöver bättre kunskap om internetsäkerhet och är medveten om riskerna efter att ha hört om vänner som blivit drabbade.

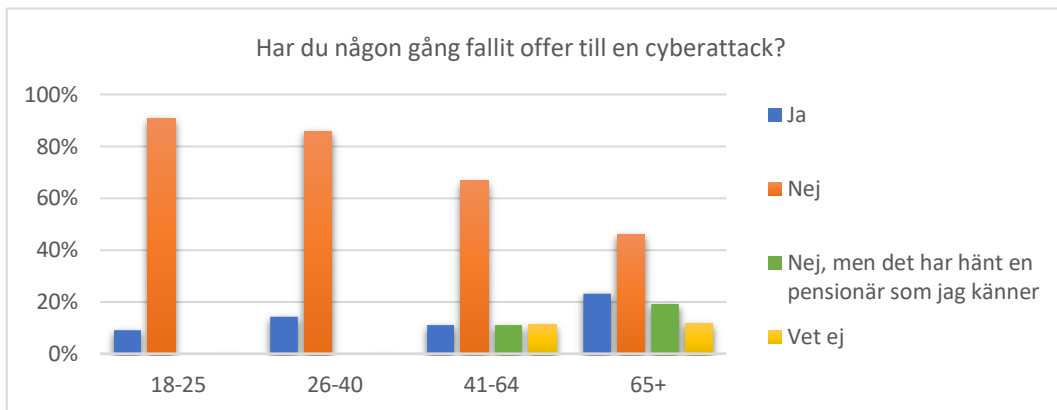
5. Analys

I figur 13 framgår det att majoriteten av respondenter inom åldrarna 18–64 föredrar digitala tjänster framför icke-digitala, vilket avviker sig från resultaten från de respondenternas i åldersgruppen 65+ (65 år och äldre). Där finns det en 60–40 fördelning med 60% som valde icke-digitala tjänster och 40% som valde digitala. Detta mönster stöds relativt av forskning som refererats till tidigare i denna studie (Holgersson et al., 2023), vilket indikerar en rädsla bland många pensionärer för digitala miljöer. Som sagt föredrar vissa fortfarande att använda digitala alternativ inom denna åldersgrupp, vilket ytterligare exemplifieras av den 65-årige man som intervjuades till studien.



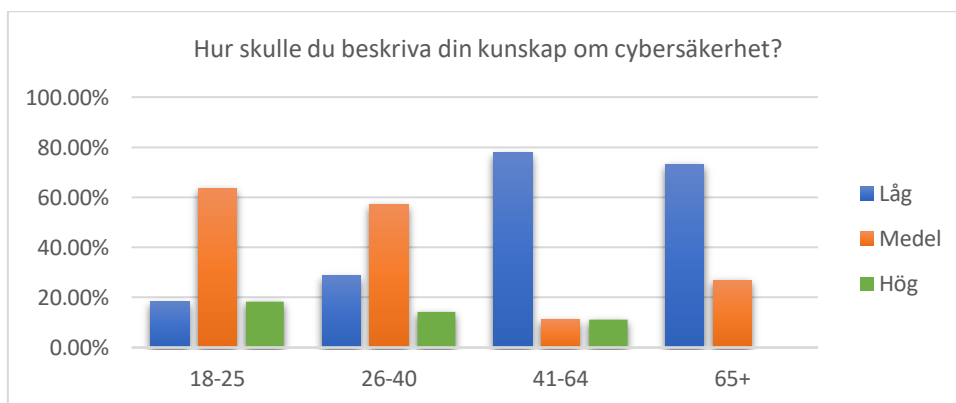
Figur 13, digitala tjänster: ålder

Denna dynamik inom den äldre befolkningen kan delvis förklaras av en ökad medvetenhet om cyberbrott, vilket framgår av resultaten i figur 14. Även om majoriteten av pensionärerna ej har blivit offer för cyberattacker visar data att denna åldersgrupp är mer spridd i sina erfarenheter och uppfattningar om cyberhot jämfört med yngre åldersgrupper.



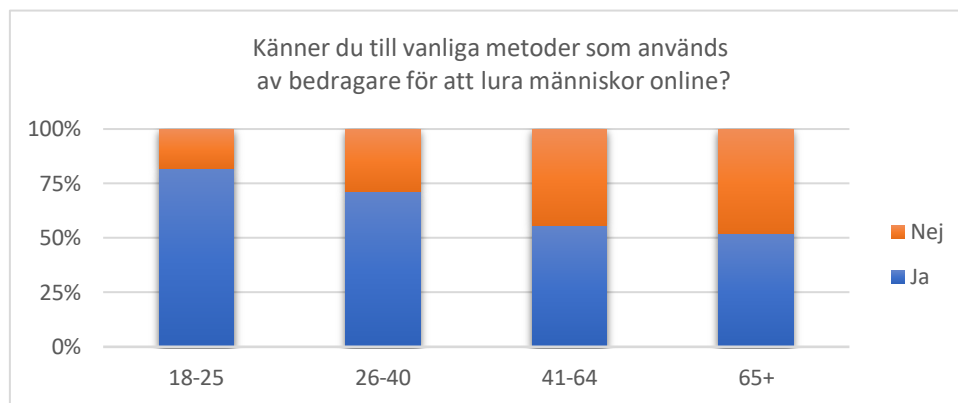
Figur 14, cyberattack offer: ålder

När det gäller självreflekterad kunskap om cybersäkerhet uppstod det variation mellan mitten av åldersfördelningen, där åldersgrupperna 18–25 och 26–40 bägge mestadels kände att sin kunskap inom cybersäkerhet var medel i nivå, medan åldersgrupp 41–64 respektive 65+ kände sin kunskap ligga på låg nivå.



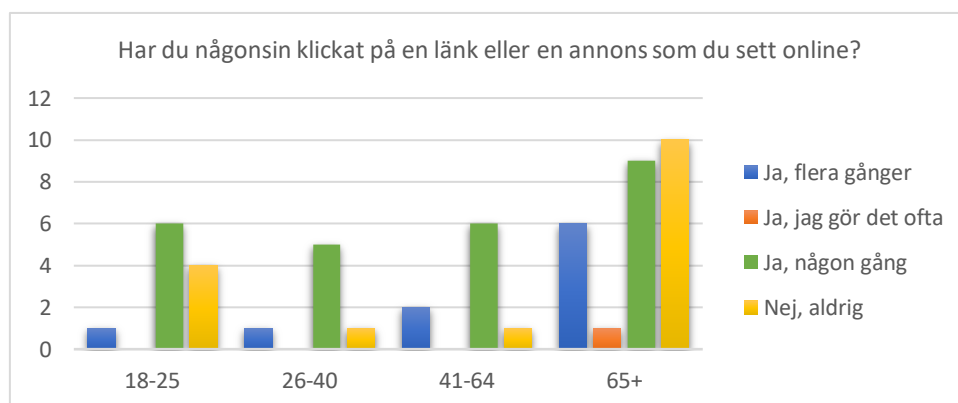
Figur 15, cybersäkerhet kunskap: ålder

Gällande kunskap inom de flera bedrägerimetoder som används online visar figur 16 att det finns ett mönster med ålder. Desto äldre respondenterna var, desto högre chans var det att de ej visste om dessa metoder. Argumentet för bristen av kunskap och information stärks även av figur 15 där vi ser en trend av äldre personer med låg kunskap av cybersäkerhet. Det stärks ytterligare av den 23-årige intervjupersonen, respondent 2, där de har en grundläggande förståelse över cybersäkerhet och de metoder som bedragare använder för att få tag på användarens information, då de känner folk som har blivit offer till det.



Figur 16, kunskap om bedrägerimetoder: ålder

Figur 17 visar ett samband till figur 14 där svaren från respondenterna inom åldersgruppen 65+ har en större utspridning än de andra åldersgrupperna. Figur 16 visar även att åldersgruppen 65+ är mer oroad och rädda för vad som kan hända om de så klickar. Som Holgersson et al. (2023) antyder i sitt papper är många pensionärer rädda att använda internet utanför vad de är bekväma med.



Figur 17, annonser och länkar: ålder

6. Diskussion

Analysen av denna studie indikerar att det finns en märkbar brist på kunskap och medvetenhet om cybersäkerhet bland äldre, vilket gör dem till en sårbar grupp för cyberbrott. Trots att många pensionärer använder internet och digitala tjänster regelbundet, är det tydligt att de känner en osäkerhet kring hur de ska skydda sin personliga information online. Detta framgår av både enkätresultaten och intervjuerna, där många respondenter uttrycker en önskan om mer utbildning och stöd inom området.

Ett av de mest märkbara resultaten är att en betydande andel av pensionärerna föredrar icke-digitala tjänster jämfört med de yngre åldersgrupperna, vilket tyder på en viss grad av digital rädsla eller osäkerhet. Detta kan delvis förklaras av den bristande kunskapen om cybersäkerhet, men också av en generell oro för att bli lurad eller utsatt för bedrägeri online. Denna oro är inte helt obefogad, då äldre ofta utgör en målgrupp för cyberbrottslingar som utnyttjar deras brist på digital erfarenhet.

Trots att studien har identifierat dessa trender och mönster, är det viktigt att ifrågasätta och reflektera över dess resultat. Urvalet av respondenter var begränsat både i antal och geografisk spridning, vilket kan ha påverkat generaliserbarheten av resultaten. Det faktum att en majoritet av de svarande var män kan också ha påverkat resultaten, eftersom kön kan spela roll i hur man upplever och hanterar cybersäkerhet.

En annan begränsning av studien är den relativt korta tidsramen för datainsamling, vilket kan ha begränsat möjligheten att nå en bredare och mer representativt urval av äldre vuxna. Dessutom kan utformningen av vissa enkätfrågor ha påverkat respondenternas svar och därmed resultaten av studien. Exempelvis var vissa frågor kanske inte tillräckligt nyanserade för att fånga upp alla aspekter av respondenternas erfarenheter och uppfattningar.

Framåt är det viktigt att utveckla och implementera specifika utbildningsprogram som är anpassade för äldre och deras behov. Dessa program bör inte bara fokusera på tekniska aspekter av cybersäkerhet, utan även på att bygga en grundläggande förståelse och tillit till digitala tjänster. Genom att involvera äldre i utvecklingen av dessa program kan man säkerställa att de är relevanta och effektiva.

7. Slutsats

7.1. Slutsatser

Undersökningen har bidragit till en fördjupad förståelse av äldres kunskaper och upplevelser av cybersäkerhet. Resultaten visar att även om många äldre använder internet och digitala tjänster dagligen, finns det en betydande brist på kunskap kring cybersäkerhet och hur man skyddar sig online. Trots att majoriteten av respondenterna inte har blivit offer för cyberbrott, anser de flesta att det finns en brist på tillräcklig utbildning och stöd för de äldre i detta avseende.

Efter att ha analyserat resultaten framkom det att äldre personer tenderar att vara mer återhållsamma med att använda digitala tjänster och föredrar icke-digitala alternativ. Denna preferens kan leda till en ökad digital skillnad mellan generationer och påverka tillgängligheten till viktig information och tjänster. Framtida forskning bör fokusera på att undersöka vilka faktorer som påverkar äldres användning av digitala tjänster samt utveckla strategier för att öka medvetenheten och kompetensen inom cybersäkerhet bland denna grupp. Genom att utforska och adressera dessa områden kan vi arbeta mot att skapa en mer inkluderande och säker digital miljö för alla åldersgrupper.

Framtida studier bör fokusera på att utveckla och implementera utbildningsprogram som är specifikt utformade för äldre och deras behov. Dessutom är det viktigt att undersöka hur olika faktorer, som till exempel ålder och digital erfarenhet påverkar äldres förmåga att säkerställa resultatens trovärdighet och generaliserbarhet.

7.2. Metoddiskussion

Denna studie har använt mixed-methods där kvantitativa och kvalitativa metoder kombineras för att undersöka cybersäkerhet bland äldre vuxna. Metoden har möjliggjort en omfattande och nyanserad förståelse av ämnet. Mixed-methods strategi innebär att man kan triangulera data från olika källor, vilket ökar trovärdigheten i resultatet. Genom att jämföra och kombinera resultat från enkäten och intervjuerna kan vi identifiera trender och mönster samt avvikelser, vilket ger oss en mer nyanserad förståelse av ämnet. Dock medför mixed-methods också vissa utmaningar som har påverkat forskningsprocessen och resultaten.

Användningen av enkäter och intervjuer har visat sig vara effektiv för att nå en bred population och samtidigt få djupare insikter. Enkäterna gav oss möjligheten att samla in data från ett större antal respondenter, vilket ökade studiens statistiska generaliserbarhet. Samtidigt gav intervjuerna möjlighet att utforska deltagarnas individuella erfarenhet och uppfattning på ett djupare plan. Dock uppkom det problem kring dessa metoder som med mer tid och resurser kan åtgärdas för att förbättra resultaten.

Problemet som hittades med denna metod var främst på enkäten där utformningen av frågor och svarsalternativ gav undersökning data som var ej användbara. Exempel på detta är på enkätfråga 3 där det handlar om könsidentitet. Ett exempel på en fråga som kan förbättras med hjälp av bättre utformning är fråga 13 i enkäten där deltagarna frågas om deras preferens mellan digitala och icke-digitala tjänster. I frågan erbjöds endast tre svarsalternativ: "Digitala tjänster", "Icke-digitala tjänster" och "Vet ej". Detta begränsade svarsmöjligheterna och kan ha påverkat resultaten. Ett bättre tillvägagångssätt skulle ha varit att inkludera alternativ som "Ingen preferens" eller "Jag gillar båda lika mycket". Detta medför en mer nyanserad bild av respondenternas preferenser.

Ett till problem som uppkom var att säkerställa ett tillräckligt stort och representativt urval av äldre vuxna. Därför använde vi oss av både digitala och traditionella metoder för att nå ut till deltagarna vilket innebar att vi kunde nå äldre som ofta är mindre villiga att använda digitala verktyg. Dock fick vi in endast 53 enkätsvar och 2 intervju på grund av begränsning i vår studie vilket var tid och resurser, vilket i sin tur begränsar de slutsatser vi kan dra. Eftersom antalet deltagare var begränsat kan detta ha påverkat generaliserbarheten av resultaten. Intervjun som utfördes når även ej upp till det förväntade 45 – 60 minuter på grund av få mängd respondenter och ej noggrant utformade intervjufrågor vilket resulterade i kortare svar från respondent 1. En bredare geografisk spridning hade kunnat förbättra svarsfrekvensen och resultatens trovärdighet och fler intervjuer hade kunnat ge en mer varierande bild och stärka resultatens validitet. Sedan är det även bra att tänka på att urvalets representativitet spelar en stor roll. Om urvalet ej är representativt för den större populationen av pensionärer kan resultaten vara missvisande.

Användningen av Microsoft Forms och Excel underlättade datahanteringen och möjliggjorde effektiva analyser av enkätsvaren. Vissa tekniska problem vid

transkriberingen av intervjuer krävde noggrann manuell granskning för att säkerställa korrektheten. Detta extra steg i processen bidrog till en mer tidskrävande analys men var nödvändig för att bevara datakvaliteten.

7.3. Reflektion över den egna processen

Kring studieämnet som valdes ansågs vi vara för stor längre in i uppgiften. Att ämnets målgrupp var svårt att nå i stormängd med den tidsramen vi hade samt tillgänglighet av alla författarna resulterade i få mängd av intervju och enkätsvar.

Reflekterande över vår process, var det tydligt att en mer strukturerad tidsplan och bättre fördelning av arbetsuppgifter hade kunnat förbättra effektiviteten. Kommunikations- och samarbetsverktyg användes flitigt, men ibland uppstod missförstånd kring deadlines och förväntningar. En tydligare projektledning och mer regelbundna uppföljningsmöten hade kunnat minska dessa problem. Sedan krävs det även förbättring kring att alla medlemmar är på samma sida kring förståelsen för ämnet och teorin. Missförståelse kring teorin och syftet kan resultera i att arbetet inte är anpassat efter varandra. Ett exempel är på enkätfrågor och intervjufrågor där data som samlades in gav väldigt lite till undersökning på grund av utformningen av frågorna. För att förbättra denna studie allmänt anser vi att en kritisk granskning av alla delar behövdes för alla gruppmedlemmar. För framtida arbete behövs en bättre arbetsprocess samt kommunikation mellan författarna för att kunna öka reliabilitet och validitet.

När vi bedömer trovärdigheten i våra resultat, är det viktigt att erkänna de begränsningar som vår urvalsprocess och det begränsade antalet intervjuer medför. Därför anser vi resultatets trovärdighet som relativt låg. Trots detta anser vi att våra metodval har varit passande för att lyfta fram de grundläggande frågeställningarna kring cybersäkerhet och äldre. Kombinationen av kvantitativa och kvalitativa metoder har möjliggjort en välförsedd och mer balanserad förståelse, även om det finns utrymme för förbättringar i framtida studier. Vi hoppas att vår inblick kan bidra till vidare forskning och praktiska åtgärder för att förbättra cybersäkerheten för äldre.

Referenser

- Appelt, L. C. (2016). *Designing for the elderly user: Internet safety training*
<https://www.proquest.com/docview/1797962439?parentSessionId=4FifKAC1Omly6reeCGXFUq0JZ6lVCt%2BRLIZZWwvQcpU%3D&pq-origsite=summon&accountid=10404&sourcetype=Dissertations%20&%20Theses>
- Brody, R. G., Mulig, E. & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal*, 11(3), 1-12
<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c3f9bedf86614a9ca7cf18197bfbb978f56e6e56>
- Björklund, M., & Paulsson, U. (2012) Seminarieboken: att skriva, presentera och opponera (2 uppl.). Studentlitteratur.
- Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology*, 36(3), 173-192.
<https://doi.org/10.1080/03601270903183065>
- Holgersson, J., Kävrestad, J., & Nohlberg, M. (2021). *Cybersecurity and Digital Exclusion of Seniors: What Do They Fear? Human Aspects of Information Security and Assurance*, 12–21.
https://doi.org/10.1007/978-3-030-81111-2_2
- Holgersson, J., & Söderström, E. (2019). Bridging the gap: Exploring elderly citizens' perceptions of digital exclusion. Proceedings of the 27th European Conference on Information Systems (ECIS). Presented at the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden, June 8-14, 2019. Hämtad från
<http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-16908>
- Lindholm, C (u.å.). Cybersäkerhet, I Nationalencyklopedin. Hämtad 01-05-2024 från
[cybersäkerhet - Uppslagsverk - NE.se](https://www.encyklopedin.se/cybersakerhet)
- Möller, P.F., Dietmar. (2023). *Guide to Cybersecurity in Digital Transformation*. Springer Cham. <https://doi-org.www.bibproxy.du.se/10.1007/978-3-031-26845-8>
- Nationalencyklopedin (u.å.). Spam. Hämtad 26-05-2024 från <https://www-encyklopedi1999.www.bibproxy.du.se/uppslagsverk/encyklopedi/l%C3%A5ng/spam>

Bilaga 1: Missivbrev till Enkät

”Vi är tre studenter från Högskolan Dalarna som undersöker den allmänna kunskapen kring cybersäkerhet bland pensionärer.

Tack så mycket för att du tar dig tid att delta i vår enkät. Enkäten tar ungefär 5 minuter att genomföra och är helt anonym.

Författare: Ali Adrian Nasrat, Vilmer Skoglund, Porsche Thichan”

Se fråga 1 i enkätformulär för samtycke.

Bilaga 2: Enkätformulär

- 1. Samtycker du om att svaren i enkäten används till en undersökning i en studie?**

(Alla svar är totalt anonyma) *

Ja

Nej

- 2. Hur gammal är du? ***

Under 18

18–25

26–40

41–64

65+

- 3. Vad är din könsidentitet? ***

Man

Kvinna

Annat

Vill ej ange

- 4. Hur ofta använder du internet eller digitala tjänster? ***

Någon gång om året

Någon gång i månaden

Någon gång i veckan

Flera gånger i veckan

- 5. Hur säker känner du dig när det gäller att hantera personlig information online?**

(Adress, bankinformation, telefonnummer, m.m.) *

Mycket osäker

Osäker

Något säker

Säker

- 6. Har du någonsin delat dina bankuppgifter eller personlig information med någon online utan att först verifiera att det var en legitim källa? ***

Ja

Nej

Vet ej

- 7. Har du någonsin klickat på en länk eller en annons som du sett online? ***

Ja, jag gör det ofta

Ja, flera gånger

Nej, aldrig

Vet ej

8. Har du någonsin fallit offer för en phishing-attack online?

(Phishing är när bedragare använder falska e-postmeddelanden, texter eller webbplatser för att lura folk att dela sina personliga eller finansiella uppgifter) *

Ja

Nej

Nej, men det har hänt en pensionär jag känner

Vet ej

9. Känner du till vanliga metoder som används av bedragare för att lura människor online?

(Exempel: phishing, skräppost, falska webbplatser) *

Ja

Nej

Vet ej

10. Har du någonsin fått utbildning eller information om cybersäkerhet och hur man skyddar sig mot cyberattacker? *

Ja

Nej

Vet ej

11. Tycker du att det finns tillräckligt med stöd och tillgänglig utbildning om cybersäkerhet för dem som behöver det? *

Ja

Nej

Vet ej

12. Hur skulle du beskriva din kunskap om cybersäkerhet? *

Låg

Medel

Hög

13. Föredrar du generellt att använda digitala tjänster eller icke-digitala tjänster?

(Exempel: Handla kläder via en webbsida eller i en butik) *

Digitala tjänster

Icke-digitala tjänster

Vet ej

14. Om du valde icke-digitala tjänster i frågan ovan, varför?

Ange ditt svar:

Bilaga 3: Missivbrev till Intervju

Hejsan!

Vi är tre studenter från Högskolan Dalarna som genomför en studie om den allmänna kunskapen kring cybersäkerhet bland pensionärer. Vi söker nu ut personer att intervjua till denna studie och undrar om du skulle vara intresserad att delta.

Under intervjun kommer vi att ställa frågor kring cybersäkerhet och din upplevelse kring ämnet. Du har rätten att vara helt anonym om du så vill. Om du väljer att förbli anonym kommer endast uppgifter om din ålder och könsidentitet att samlas in och inkluderas i studien. Om du däremot väljer att ej förbli anonym kommer uppgifter som din ålder och könsidentitet samt fulla namn att inkluderas i studien.

Studien kommer ej att publiceras någonstans, och kommer endast bli sedd av studenter och lärare på kursen *Forskningsmetodik* på Högskolan Dalarna

Genom att delta i intervjun samtycker du till att samtalet spelas in och sedan transkriberas, samt att dina svar används i undersökningen.

Med vänliga hälsningar,
Ali Adrian Nasrat, Vilmer Skoglund, Porsche Thichan
Studenter vid Högskolan Dalarna

Bilaga 4: Intervjuformulär

Fråga 1. Hur gammal är du?

Fråga 2. Hur ofta använder du internet?

Fråga 3. Har du någonsin fått eller deltagit i en utbildning eller kurs som handlar om internetsäkerhet?

Fråga 4. Har du någonsin tryckt på en länk eller annons online?

Fråga 5. Har du någonsin blivit utsatt för någon form av cyberattack?

Fråga 6. Tar du några åtgärder för att skydda dig själv online, exempelvis olika lösenord, två faktor autentisering eller antivirusprogram?

Fråga 7. Föredrar du generellt att använda digitala eller icke-digitala tjänster. Exempelvis att läsa nyheter på en hemsida eller i en tidning

Fråga 8. Känner du att information och kunskap inom internetsäkerhet kan förbättras för din generation?

Bilaga 5: Transkribering av intervju(er)

Respondent 1:

Hej innan intervjun börjar så vill jag informera dig om vad intervjun kommer handla om. Frågorna kommer att handla om cybersäkerhet. Dina svar kommer att vara anonyma och du får avbryta när som helst. Har jag ditt samtycke att genomföra intervjun?

Ja du har mitt samtycke.

Hur gammal är du? Och vilket kön identifiera du dig som?

Jag är 65 årig man.

Hur ofta använder du internet? Och vad använder du det till?

Jag använder internet varje dag till att kolla på Facebook, Nyheter och annat.

Har du någonsin fått eller deltagit i en utbildning eller kurs som handlar om internetsäkerhet?

Nej det har jag inte, men jag har lärt mig det mesta jag vet själv. Man har ju sett lite här och där på nätet när folk blir lurat så då har väl man sökt upp och läst lite.

Har du någonsin tryckt på en länk eller annons online?

Ja, det beror ju på vad det är. Man har ju tryckt på vissa länkar på Facebook ibland som leder till nyheter och sånt och hittills har jag inte haft nåt problem. Men om man tänker på annonser när man är inne på en webbsida så har jag inte tryckt.

Har du någonsin blivit utsatt för någon form av cyberattack?

Nej, det har jag inte. I alla fall inte vad jag vet om.

Tar du några åtgärder för att skydda dig själv online, exempelvis olika lösenord, två faktor autentisering eller antivirusprogram?

Ja delvis. Olika lösenord har jag inte. Det blir för svårt att komma ihåg. Två faktor autentisering vet jag inte vad det är.

Det är när man till exempel får ett sms eller bekräftelsemejl när du själv logga in på en ny enhet. Alltså att du får själv bekräfta att det är du som loggar in så att i ett fall där du inte loggar in men får ett meddelande eller bekräftelsemejl så kan du neka inloggningen eftersom det är inte du som har försökt logga in.

Jaså, ja då har jag det för jag har fått sms och mejl ibland när jag ska logga in på någonstans. Även antivirusprogram har jag på min dator.

Hur har du lärt dig att man kan använda ett antivirusprogram då?

Det kommer jag inte riktig ihåg, men det lär väl bara vara nåt som man själv lärde från. Det brukar ju installera ett antivirusprogram automatiskt ibland när man köper en ny dator.

Föredrar du generellt att använda digitala eller icke-digitala tjänster. Exempelvis att läsa nyheter på en hemsida eller i en tidning?

Jag föredrar digitala. Det är smidigare och jag slipper ha massa tidnings papper.

Föredrar du det även när det gäller att handla saker?

Ja, det gör jag. Jag beställer ganska mycket hem. Men i för sig så handlar jag inte digitalt när jag ska handla mat så där är det väl lite upp till vad man köper.

Men du känner dig säker när du ska handla saker online? Alltså när det kommer till att skriva in bankinformation.

Jaaaoo, Det är beror ju lite på vart man handla. Köper jag från Elgigantens hemsida så är jag ju ganska säker men om det är en sida som jag inte känner igen så undviker jag ju de.

Känner du att information och kunskap inom internetsäkerhet kan förbättras för din generation?

Ja det tycker jag. Man skulle ha haft fler gratis utbildning eller bara allmänt öppet tips och råd när det kommer till sånt. Jag känner ju många som inte vet så mycket om internetsäkerhet och för de så skulle det var till stor nytta om de kunde veta lite mer. Problemet just nu är att det finns skydd men vi gamla människor fattar inte förklaringen till vad de är. Det är för komplicerat ord och det skulle vara bättre om det kunde förklaras på ett lättare sätt.

Respondent 2.

Intervjuaren: Hejsan, välkommen till intervjun. Först vill jag förklara vad denna intervju kommer ställa för frågor.

Anonym: Jadå.

Intervjuaren: Intervjun kommer att fokusera på frågor om cybersäkerhet. Innan vi börjar behöver jag först fråga om ditt samtycke för att spela in denna intervju och att intervjun används till min grupps studie.

Respondent 2: Jag samtycker.

Intervjuaren: Du har också rätten att vara anonym i studien om du så vill.

Respondent 2: Ja det kan jag vara tack!

Intervjuaren: Vad bra! Då kan jag börja med att fråga två bakgrundsfrågor. Hur gammal är du, och vilken könsidentitet har du?

Respondent 2: Jag är en 23 årig man.

Intervjuaren: Ja, då kommer vi till första intervjufrågan. Hur ofta använder du internet?

Respondent 2: Oj. Ja, det är väl dagligen. Flera gånger om dagen alltså.

Intervjuaren: Och har du någonsin fått eller deltagit i en utbildning eller kurs som handlar om internetsäkerhet?

Respondent 2: Nej, det har jag aldrig gjort.

Intervjuaren: Har du någonsin tryckt på länk eller annons online?

Respondent 2: Ja jo, jag har tryckt på några länkar förut.

Intervjuaren: Och, har du känt att någonting kan hända inom cybersäkerhet. Till exempel, har du känt dig säker att trycka på dem, liksom har du bara tryckt utan att tänka på det?

Respondent 2: Nej, men det beror ju på vad det är för en länk. Liksom om det är en länk till en hemsida man känner igen, då vet man ju liksom. Då kan man lita på den. Men om det är

till en hemsida man inte varit inne på förut, då brukar man fundera lite innan man klickar. Likadant är det om det är någon som har skickat något till mig om man inte så här riktigt känner den personen, då tänker man ju lite extra och kanske kolla upp lite innan.

Intervjuaren: Om länken är till en sida som du känner igen, brukar du då också kolla om det är rätt länk.

Respondent 2: Alltså ja, men inte super noggrant. Jag tänker väl att man ser om det är rätt hemsida i länken. Liksom om det är en länk till en sida som vanligtvis har .com, och nu i stället har .co.m eller nåt sånt, så brukar jag inte klicka på dem. Men det kan väl hända om man är snabb.

Intervjuaren: Ja, jag förstår. Men om någon som du känner skickar något till dig, litar du alltid på det eller är du fortfarande lite skeptisk?

Respondent 2: Om det är en sida som jag inte känner igen brukar jag också vara lite skeptisk faktiskt. Jag brukar inte bara klicka på vad som helst liksom.

Intervjuaren: Ja, okej. Har du någonsin blivit utsatt för någon form av cyberattacker? Det kan vara till exempel phishing, om du vet vad phishing är.

Respondent 2: Mm, ja, men typ. Kan du förklara?

Intervjuaren: Phishing är liksom när någon försöker att ta dina uppgifter, och det kan vara personliga uppgifter eller typ banknummer, genom att låtsas att vara en bank eller något sådant via e-mail eller på något sånt sätt.

Respondent 2: Ja men precis. Alltså, man har ju fått så här e-mail och grejer. Sms har man ju också fått, alltså folk som försöker liksom lura den på såna sätt. Men jag har aldrig blivit utsatt på det sättet. Alltså jag har inte gått på det och blivit av med något så här konto eller banknummer liksom. Jag har varit med och sett det, men jag har aldrig blivit utsatt och förlorat något på det riktigt.

Intervjuaren: Alltså menar du att du har sett någon annan som du känner blivit utsatt?

Respondent 2: Nej, men jag menar, jag har liksom sett såna där meddelanden.

Intervjuaren: Ja, du menar bara att du sett e-mail och sms och sånt?

Respondent 2: Ja precis. Jag har haft möjligheten att ha blivit utsatt liksom.

Intervjuaren: Så du har aldrig gått på något sånt.

Respondent 2: Nej, nej.

Intervjuaren: Har du några åtgärder för att skydda dig själv online, exempelvis olika lösenord, två faktor autentisering, antivirusprogram, något sånt?

Respondent 2: Jo men det har jag ju. Antivirusprogram har jag. Och sen är jag lite dålig på det med lösenord. Det är kanske inte så bra att säga det.

Intervjuaren: Intervjun är Respondent 2, så det är lugnt.

Respondent 2: Ja juste. Ja, jag är väl lite dåligt på att använda olika lösenord. Jag har liksom några varianter som jag växlar mellan, så det är ju lite säkerhet. Men man skulle ju kunna vara bättre att med att ha olika lösenord till typ allting egentligen. Det är väl det bästa egentligen antar jag.

Intervjuaren: Sen har vi två faktor autentisering också. Har du något sånt?

Respondent 2: Ja, men det har jag. Alltså, det är många ställen som tvingar en till att ha det nu för tiden, så det har man. Men jag kan tycka att det är drygt ibland. Att man måste liksom varje gång du ska logga in någonstans, då måste du in på till exempel din e-mail också. Och då om det typ är via e-mail så behöver man ibland vänta ett tag på det, sen trycka en länk eller kopiera en kod och gå tillbaks när det tog mycket längre tid. Men det är ju för säkerhets skull. Så det är väl en bra grej att ha egentligen. Men om jag kan skippa det brukar jag faktiskt göra det.

Intervjuaren: Det var det jag tänkte fråga. Alltså om du väljer att skippa två faktor autentisering om du har valet att göra det?

Respondent 2: Ja, jag brukar skippa det om jag inte måste ha det, vilket kanske inte är det smartaste egentligen.

Intervjuaren: Beror det på olika orsaker. Till exempel om det är kanske ditt e-mail konto eller något sånt där, eller Youtube konto. Brukar du då använda det?

Respondent 2: Nej, eller alltså det beror ju på om det är för någonting viktigt som sagt då, då brukar jag väl använda det liksom.

Respondent 2: Vad anser du som viktigt i så fall?

Intervjuaren: Ja egentligen det viktigaste är ju typ ens e-mail. Och ja, det är typ det. E-mail till Google konto och så där. Annars om det bara är alltså till någon profil på någon hemsida då kvittar liksom, känner jag. Då vill jag bara kunna logga in liksom.

Intervjuaren: Så där är det mer prioritering på att vara smidigt och snabbt, och det kanske blir lite segt att använda tvåfaktor då kanske?

Respondent 2: Ja jo, men det tycker jag. Det är som jag skulle använda McDonalds appen en gång. Jag stod liksom vid McDonalds och skulle använda appen och då hade den loggat ut mig. Och då sa den att jag behövde logga in i McDonalds appen. Alltså skriva in allting, och då måste jag in på min e-mail för att hämta någon kod och liksom skriva in också. Och det är liksom. Jag vet inte alltså, det är liksom min McDonalds app. Jag bryr mig inte så mycket om säkerhet där. Vid typ såna tillfällen hade jag bara hellre inte haft två faktor grejen.

Intervjuaren: Så du tänker om de kanske om någon skulle ta det? Alltså "vem skulle ens försöka ta kontot" liksom?

Respondent 2: Ja precis vem vill in på min McDonalds. Typ att någon försöker phisha mig för att få McDonalds kontot. Typ att de tar mina erbjudanden eller nåt.

Intervjuaren: Ja, haha. Men skulle du känna dig osäker om ditt McDonalds konto blev hackad eller att någon hade stulit din inloggning?

Respondent 2: Alltså jag skulle väl typ inte bry mig så mycket, det är ju inte riktigt något viktigt konto. Fast jag skulle nog vara lite skeptisk ifall min e-mail också var hackad eller något, men i så fall skulle inte veta varför de gick in i min McDonalds app haha. Eller ja, kanske om ja har typ samma lösenord på den appen som är ansluten till min e-mail, men ja vet inte om jag skulle tänkt på det om det hände på riktigt.

Intervjuaren: På tal om det här med olika lösenord. Känner att du dig sårbar eftersom du har typ samma lösenord eller kanske några stycken bara som du använder?

Respondent 2: Alltså, man har ju tänkt på det ibland. Det känns ju lite dumt att ha samma lösenord till allt liksom. Men det är därför jag brukar ha ett mycket starkare lösenord till de grejer som jag tycker är viktigare. Men då är det liksom om de får tag på ett av dem då kommer de in på alla. Men sedan har jag liksom andra lösenord till andra grejer som är som

inte är lika så viktiga. De kan bli komplicerat. Så anledningen att jag inte har fler lösenord är väl egentligen att det blir väldigt svårt att komma ihåg alla liksom. Då är alternativet att skriva ner det någonstans, men då är man skriver ner alla lösenordet någonstans, typ om vi säger att jag skriver ner alla lösenord i mobilen någonstans. Om någon då får åtkomst till min mobil, då kan de säga alla mina lösenord. Om jag annars typ skriver det på en lapp någonstans och lägger den i, ja, jag vet inte, typ mitt rum i typ någon låda. Då kanske jag tappar bort den i stället. Då vet man inte vart den är. Den kan ju ha hamnat typ vart som helst. Eller så kan vem som helst bara gå in i mitt rum och om dem hemma hos mig, och få på tag på allting liksom.

Intervjuaren: Ja, jag förstår. Använder du någonsin andra konton för att logga in på saker som när till exempel en sida frågar om du vill logga in med Facebook eller logga in med Google och sånt här.

Respondent 2: Andra konton? Hur menar du då?

Intervjuaren: Att på vissa hemsidor så kan man gå in och så står det bara "Logga in med Google" typ. Alltså att man kan logga in med andra slags konton.

Respondent 2: Ja, jag kan väl göra det ibland. Det är väl för det är så lätt liksom

Intervjuaren: För att det är snabbt och smidigt, eller?

Respondent 2: Ja, exakt. Men det beror ju återigen på vad det är. Alltså jag har en e-mail som jag använder till det mesta liksom. Jag har så mycket på den redan så jag använder den till allting i princip. Och sen har jag en som jag försöker hålla lite mer minimalistiskt. Liksom inte nå mycket på. Alltså mer viktiga saker. Jag använder nästan aldrig den för att logga in på grejer. Det är typ bara för att slippa få massa meddelanden och sånt på den.

Intervjuaren: Ja, jag förstår. Föredrar du generellt att använda digitala eller icke digitala tjänster, till exempel som att läsa nyheter på en hemsida mot i en tidning, eller köpa kläder online mot på en affär?

Respondent 2: Köpa kläder och sånt gör jag helst i en affär bara för att man kan prova på kläder. Det är omöjligt att veta liksom hur de passar online. Man vet liksom inte hur de ser ut eller så riktigt för man vet ju aldrig riktigt om bilderna är äkta det man ser på online och sånt. Och sen, vad var det första du sa?

Intervjuaren: Nyheter och liknande.

Respondent 2: Ja med sånt också. Ja alltså, det är också egentligen något som jag hellre gör utan internet och sånt. Alltså, det är ju smidigt att kunna söka upp vad som helst på mobilen och läsa nyheter och sånt, men jag tycker det är alltså trevligare att sitta med en tidning egentligen. Det är liksom lite mer fokuserat på något vis. Det minskar ju också skärmtiden och sånt där.

Intervjuaren: Ja, det kan jag tänka mig. Men känner du att du handlar mer i person över online i så fall?

Respondent 2: Alltså jag tror jag använder de lika mycket, men för olika saker. När jag handlar kläder och till exempel mat på ICA och sånt handlar jag ju helst i person. Men om det är typ en sak jag köper ofta, typ någon hårprodukt som har använt innan, eller om det är något sak jag hittar när jag är online, då brukar jag skicka efter det där för jag tycker det blir smidigare. Det bror väl på om jag behöver det pronto också.

Intervjuaren: Ja, jag förstår. Känner du att information och kunskap inom internets säkerhet kan förbättras för din generation?

Respondent 2: Ja, men det tror jag väl. Jag vet inte på vilket sätt riktigt för det beror ju helt på hur man är uppväxt. Liksom vad man har hållit på med när man växt upp.

Intervjuaren: Ja.

Respondent 2: För en del man träffar så har de ingen aning om sådant här, även alltså folk från min generation. Men jag har väl någorlunda koll i alla fall. Sen väljer jag lite vad jag vill bry mig i och inte ändå, men. Det beror ju som sagt på. Så det är ju definitivt inte dålig grej. Det är bara bra om fler blir upplysta. Om faror och sånt som finns online. Man har ju kompisar som man har hört blivit av med konton och sånt. Av olika former så.

Intervjuaren: Skulle du kunna expandera på det om det är någon specifik händelse du kan tänka på som du är villig att berätta om?

Respondent 2: Ja nej, man har ju haft kompisar som har blivit drabbade av sånt, men det är inte någon specifik händelse jag kan komma på. Eller jo, en kompis jag har. Han blev av med ett konto han hade på Steam med sina spel och grejer. Så han vart helt utelåst från kontot och han hade jättesvårt att fixa tillbaks det. Det var ju inte så kul när man har lagt in pengar på ett konto och sen om man spel och sånt där. Så det är ett exempel. Sen har man ju andra också, men det är inga kom ihåg så, men jag vet att det har hänt liksom. Folk har blivit av med typ andra konton. Till exempel med ett instagramkonto. Jag har jag haft en kompis som hade

blivit av med det. Det är också en sån här "scam" eller man kan säga? Då är det någon som har. Liksom de använder inte deras konton, men de gjorde ett konto som ser ut som min polares konto och laddar upp samma bilder också och då skrev de till mig att typ de behövde hjälp eller någonting liksom. Men man visste ju att det var fake. Man gick in på profilen och då var det inte någon man följde.

Intervjuaren: Ja, jag försår. Ja, men det var allt som jag hade att fråga i den här intervjun. Så då får jag tacka dig så mycket för dina svar!

Respondent 2: Ingen fara. Det är ju roligt att bidra till en studie liksom

Intervjuaren: Du får ha en fortsatt trevlig dag.

Respondent 2: Ja tack detsamma.