Uppsala universitet
Institutionen för informatik och media

Medvetenhet kring lösenordssäkerhet- och hantering

Är ålder en avgörande faktor?

Josefin Angerbjörn

Kurs: Examensarbete
Nivå: C
Termin: VT22
Datum: 220614

Sammanfattning

Allt mer av vår tillvaro sker i den digitala sfären och detta ställer krav på en medvetenhet kring lösenordssäkerhet- och hantering. Äldre och pensionärer är i större utsträckning sällananvändare eller använder aldrig internet och detta på grund av att de exempelvis tycker att tekniken är för krånglig eller att internet är för otryggt. Det är viktigt att äldre inte hamnar i ett digitalt utanförskap på grund av detta och därför bidrar den här undersökningen till att skapa förståelse kring detta med en jämförelse mellan hur äldre och yngre ser på lösenord och hanteringen av dessa. Detta då lösenord och hur man hanterar dessa är en stor del i användandet av internet och informationssystem. Syftet med studien är att ta reda på om det finns skillnader i medvetandet kring lösenordssäkerhet och lösenordshantering mellan äldre och yngre och en enkätundersökning skickades därför ut. När undersökningen var avslutad delades deltagarna in i två åldersgrupper. En statistisk analys med Chi Square-metoden och Fisher's Exact Test genomfördes för att se om det fanns statistisk signifikans mellan de två åldersgrupperna i de olika frågor som enkäten tog upp. Resultatet visar på signifikans i 3 av 13 frågor och en viss skillnad mellan grupperna finns därmed i ämnet.

Nyckelord

lösenordssäkerhet, säkra lösenord, CIA, lösenordshantering, lösenordshanterare, tvåfaktorsautentisering, äldre, pensionärer

Innehållsförteckning

1 Inledning

I inledningen behandlas bakgrunden till uppsatsens ämne samt en problembeskrivning som sedan landar i ett syfte med tillhörande forskningsfrågor. Vidare behandlas också uppsatsens avgränsningar samt vilka som kan tänkas vara kunskapsintressenter och ett kort avsnitt om uppsatsens disposition.

1.1 Bakgrund

I en värld där allt mer av våra liv utspelar sig på nätet blir det också allt större risk att bli utsatt för någon typ av attack mot den personliga informationssäkerheten. Enligt Internetstiftelsens senaste rapport Svenskarna och Internet 2021 (2021, s.113) har 40% av alla som är 16 år och uppåt blivit utsatta för någon form av nätbedrägeri. Det kan handla om att en obehörig exempelvis har bett personen att logga in med sitt BankID, att en obehörig använt personens kortuppgifter eller att man fått olika bluffmejl där avsändaren försöker lura till sig personuppgifter eller liknande. (Internetstiftelsen, 2021, s.113) Detta ställer krav på att människor har en vetskap kring vad som är bedrägeri och inte och hur man säkert förhåller sig till ett digitalt liv.

I Internetstiftelsens guide "Skydda dig mot bedragare" (2016, s.42-47) listas de viktigaste åtgärderna att vidta för att att uppnå en grundläggande it-säkerhet. Inledningsvis finns en uppmaning att använda säkra lösenord. Att välja säkra lösenord är något man enkelt kan göra själv och det är inte speciellt krångligt. Det krångliga handlar kanske istället om att hålla reda på alla olika lösenord man använder sig av. Det går ju sällan en dag utan att man skriver in ett lösenord någonstans. Det kan handla om att logga in på arbetsdatorn, i ett särskilt system för arbete eller studier eller kanske bara på ett socialt medium. Ett sådant utbrett användande av många olika lösenord ställer också krav på hanteringen av dessa. De diskussioner som under de senaste åren förts kring att förstärka datorsäkerhet och säkerhet i informationssystem har dock handlat mycket om mjuk- och hårdvarulösningar och väldigt lite om den mänskliga aspekten (Almehmadi och Alsolami, 2019). Flera tidigare studier, bland annat Duggan, Johnson och Grawemeyer (2012), har visat på att människan och hur den interagerar med datasystem kan ses som den svagaste länken i en säkerhetsaspekt och att många skapar svaga, förenklade och korta lösenord. Dessa lösenord tenderar också att återanvändas på flera ställen då användaren vill behöva memorera färre lösenord än nödvändigt. Även Mayer och Volkamer (2018) menar att människor idag behöver fler lösenord än de själva kan hantera. Användare hanterar enligt dem i vissa fall sina lösenord ovetande om de viktiga säkerhetsaspekter som finns och baserat på ett antal vanliga missuppfattningar om lösenordssäkerhet. En sådan missuppfattning kan exempelvis handla om att inkluderingen av siffror automatiskt gör ett lösenord mer säkert eller att inkluderingen av ett ord på ett annat språk än användarens modersmål skulle göra ett lösenord mer säkert.

1.2 Problemområde

Att människor har brist på kunskap kring vad som gör ett lösenord säkert och hur man bör konstruera och hantera sina lösenord framgår tydligt av tidigare forskning i ämnet. Vad som däremot saknas när man undersöker tidigare forskning är huruvida någon speciell åldersgrupp är mindre insatt än andra när det handlar om den personliga informationssäkerheten. I Internetstiftelsens rapport (Internetstiftelsen, 2021, s.15) finns en undersökning kring hur ofta olika grupper i samhället använder sig av internet. Enligt denna undersökning är det främst pensionärer som sällan eller aldrig använder internet. I gruppen "pensionärer" är 15%

sällananvändare och 20% använder aldrig internet. Detta kan ställas i kontrast till gruppen 16 år och äldre, där dessa pensionärer även ingår, och där bara 4% är sällananvändare och det är 6% som aldrig använder internet. Dessa siffror visar på att pensionärer totalt sett mer sällan använder sig av internet än övriga åldrar. I Svenskarna och Internet 2021 (Internetstiftelsen, 2021, s.17) finns ytterligare en undersökning kring vad dessa tidigare nämnda sällananvändare ser som störst anledning till att inte använda internet så ofta. Störst andel är 75% som anger att de inte har något behov, därefter är det 20% som angett att det är för krånglig teknik följt av 19% som har angett anledningen att internet är för otryggt. Som tidigare nämnt var många av sällananvändarna pensionärer och vi kan därför anta att ovanstående anledningar till att inte använda internet i allra högsta grad gäller dem. Medelpensioneringsåldern år 2021 var i Sverige 64,9 år (Pensionsmyndigheten, 2022) och en pensionär kan därmed antas vara en person som avrundat till heltal är 65 år och äldre. Teknologin går framåt i en hög fart (Ahmed et al., 2017, s.1) och mer och mer av våra liv sker i den digitala sfären. Viktigt är att de som är lite äldre inte går miste om viktiga samhällsfunktioner eller möjlighet till sociala sammanhang på grund av att man känner sig otrygg eller att tekniken är för krånglig. Studien ska därför bidra till att visa mönster kring dessa lite äldre människors syn på digital säkerhet där lösenord och hur man hanterar dem är en central del. Detta ska göras genom en jämförelse kring hur människor under 65 år och människor som är 65 år och äldre hanterar det som tidigare nämnts som en av de viktigaste faktorerna för att uppnå informationssäkerhet privat, vilket är användandet av starka lösenord och en god lösenordshantering.

1.3 Syfte och forskningsfrågor

Syftet med den här uppsatsen utmynnar alltså i att undersöka huruvida ålder har en inverkan på individers medvetenhet kring lösenordssäkerhet och hanteringen av lösenord. Tidigare forskning visar tydligt på bristen av kunskap och medvetenhet inom detta område men inte *hur* eller *om* äldre eller yngre användare skiljer sig åt. Förhoppningsvis kan vidare forskning inom detta resultera i svar på om så är fallet och i så fall bidra med fakta för att kunna arbeta vidare med attityder kring lösenordssäkerhet och lösenordshantering för att fler och fler ska stärka sin personliga informationssäkerhet.

Den forskningsfråga som står centralt i uppsatsen är därmed:

- Finns det skillnader i medvetenheten kring lösenordssäkerhet- och hantering mellan äldre och yngre och vilka är de i så fall?

1.4 Avgränsningar

Uppsatsens ämne kommer att begränsas till människors syn på och attityd till lösenordssäkerhet- och hantering i olika åldrar. Termen lösenordssäkerhet används för att beskriva vad som är viktigt att tänka på i utformandet av lösenord och åtgärder att vidta för att åstadkomma säkra lösenord. Termen lösenordshantering används för att beskriva hur man faktiskt hanterar sina lösenord och då exempelvis hur man förvarar dem. En avgränsning görs i hur attityderna och medvetenheten ser ut. Studien visar inte på varför deltagarna gör eller inte gör på ett visst sätt utan bara hur de gör. Detta då syftet med uppsatsen som sagt är att visa på attityder kring dessa frågor och inte på varför människor gör som de gör.

1.5 Kunskapsintressenter

Förhoppningen är att studien ska bidra med ytterligare insikter kring människors attityder kring säkra lösenord och lösenordshantering. Studien bör bidra till en förståelse för hur både yngre och äldre resonerar kring lösenordssäkerhet och hanteringen av lösenord och även upplysa om eventuella skillnader mellan de två gruppernas uppfattning.

Intressenter för denna undersökningen bör finnas inom den akademiska sfären där studien förhoppningsvis kan vara med och lägga grund för vidare forskning inom ämnet kring människors attityder kring lösenord och hanteringen av dessa. Intressenter bör också finnas i det vardagliga livet där den förhoppningsvis kan vara med och bidra till både deltagarnas och deras bekantas medvetenhet kring hur man gör för att uppnå god lösenordshantering i sitt privatliv. Slutligen bör intressenter även finnas i viss mån i näringslivet där det också är viktigt att arbeta med attityder kring dessa områden. Det finns en utbredd digitalisering inom såväl privatlivet som arbetslivet som ställer krav på en medvetenhet kring och god hantering av lösenord.

1.6 Disposition

Uppsatsens disposition ser ut som följer: 1. Inledning, 2. Teori, 3. Metod, 4. Resultat, 5. Analys samt 6. Avslut.

I inledningen ges en bakgrund till ämnet och det nuvarande forskningsläget. Där formuleras även en problembeskrivning och ett syfte för uppsatsen. I avsnittet för teori redogörs det för aktuella begrepp, tidigare forskning inom ämnet och ramverk som förekommer i uppsatsen. Metoddelen innehåller den övergripande forskningsstrategin och inom vilket forskningsparadigm studien sker. De tillvägagångssätt som används för datainsamling och urval beskrivs även här. I kapitel fyra presenteras resultatet av den insamlade datan vilken sedan analyseras i kapitel fem. Slutligen förs en diskussion kring resultatet och analysen av det i kapitel sex, avslut, där det även tas upp förslag på vidare forskning av ämnet.

2 Teori

Följande kapitel behandlar inledningsvis begreppsdefinitioner som är relevanta för uppsatsens innehåll. Fortsättningsvis behandlas tidigare forskning inom områden som uppsatsen behandlar och slutligen presenteras det ramverk som inkluderas i den här studien.

2.1 Begrepp

Följande avsnitt är en begreppsdiskussion kring olika begrepp som är viktiga att definiera för att uppsatsens innehåll ska vara lättförståeligt och tydligt.

2.1.1 Lösenordssäkerhet

Det finns olika sätt att vidta en god lösenordssäkerhet. En medvetenhet kring vad som gör ett lösenord säkert när det handlar om uppbyggnad och tecken är viktigt. Att ha en god hantering av lösenord är också vitalt för detta. Ett starkt lösenord kännetecknas av flera faktorer. Exempelvis bör ett lösenord inte innehålla någon form av personlig information såsom namn, adresser eller namn på husdjur (Bain et al., 2010 s.257) för att nämna några. Använder man sig av ord som kan kopplas till ens egen person blir det lätt för utomstående att gissa sig till lösenordet. Ett lösenord ska inte heller innehålla ord från en ordbok (Bain et al., 2010 s.257), dessa ord är också lätta att knäcka för någon som vill hacka dem. Lösenord bör vara konstruerade av en kombination av olika bokstäver, tecken och siffror (Bain et al., 2010 s.257). Längden på ett lösenord bör enligt vissa vara mellan 7-15 tecken (Bain et al., 2010 s.257) och enligt andra minst 8 tecken där 3 av dessa är specialtecken och resten är alfanumeriska tecken (Ma et al., 2010, s.586). Det viktiga verkar dock vara att använda slumpmässiga kombinationer i lösenordet.

Det är inte bara hur man konstruerar lösenordet och hur långa och komplexa lösenord man väljer som spelar roll för att vidta en god lösenordssäkerhet. Det som också spelar roll är hur man använder dem. I en studie av Ion et al., (2015, s.338) tillfrågades experter med minst 5 års erfarenhet av att läsa eller arbeta med IT-säkerhet om vad som var viktiga aspekter inom IT-säkerhet. Många av experterna i studien menade att det viktigaste inom IT-säkerhet är att ofta installera mjukvaruuppdateringar, men också att använda sig av tvåfaktorsautentisering och lösenordshanterare. De två sistnämnda går tydligt att koppla till lösenordssäkerhet och hanteringen av lösenord. Många experter menar också att det är viktigt att inte återanvända lösenord på flera ställen (Bain et al., 2010 s.257). Om en användare har samma lösenord på flera ställen kan en hacker som kommer åt ett av dessa ställen sedan ha möjlighet att ta sig in på andra ställen (Ives et al., 2004, s.76).

Sammanfattningsvis är det inom lösenordssäkerhet viktigt att både konstruera starka lösenord där personlig information eller vanliga ord ska undvikas att användas. Det är också viktigt att använda unika lösenord på olika sidor och därmed undvika att återanvända lösenord. Att använda sig av en lösenordshanterare och tvåfaktorsautentisering är också konstaterat som viktigt i sammanhanget.

2.1.2 Lösenordshanterare

En lösenordshanterare är en mjukvara som tillåter användaren att komma ihåg ett starkt huvudlösenord som används för att dekryptera användarens databas med andra lösenord (Gasti och Rasmussen, 2012, s.770). En lösenordshanterare har potential att eliminera problemet med att minnas flertalet andra lösenord då den lagrar användarens lösenord på ett

säkert sätt och möjliggör för denne att få åtkomst till dem vid behov (Kamat et al., 2018, s.23). Man behöver alltså bara minnas ett lösenord för att få åtkomst till sina andra lösenord och gör därför att användaren inte behöver minnas alla sina lösenord utan bara ett av dem. Huvudlösenordet behöver inte vara i textform utan kan även vara biometriskt, eller en kombination av båda där lösenordshanteraren istället för eller i kombination med ett vanligt lösenord (Kamat et al., 2018, s.25) använder sig av exempelvis fingeravtrycksavläsning eller ansiktsigenkänning för att få åtkomst till lösenorden. Man kan argumentera för att en lösenordshanterare i de flesta fall även använder sig av tvåfaktorsautentisering då den inte bara kräver ett huvudlösenord eller en biometriskt faktor utan också att man har faktiskt tillgång till enheten där lösenordshanteraren är installerad.

Det finns olika typer av lösenordshanterare. Vanligt förekommande är exempelvis sådana som är förinstallerade i en enhets mjukvara. Ett exempel på en sådan är iCloud Keychain (Apple Inc, 2022) som finns i Apples mjukvara iOS och som möjliggör att användaren synkroniserar lösenorden mellan sina enheter såsom dator, mobil och surfplatta. Lösenordshanteraren kan också vara inbyggd i olika webbläsare där exempelvis Google Chrome och Firefox (Zhao et al., 2013, s.448) lagrar lösenorden direkt i webbläsaren. Andra exempel är sådana som användaren själv väljer att installera och kan då vara i form av en app eller ett program som installeras på exempelvis mobilen, surfplattan eller datorn. Lösenordshanteraren kan fungera så att den lagrar lösenorden antingen lokalt i enheten, "i molnet" eller i en hybridlösning mellan dessa två (Kamat et al., 2018, s.25). KeePass (Reichl, 2022), Dashlane (DashLane Inc, 2022) och LastPass (LastPass US, 2022) är exempel på dessa respektive kategorier (Kamat et al., 2018, s.25).

Definitionen av en lösenordshanterare är alltså ett program som är förinstallerat på eller som installeras aktivt av användaren på en enhet såsom en dator, mobil eller surfplatta och som hjälper användaren att lagra och hantera sina lösenord. Detta görs genom att användaren loggar in i lösenordshanteraren med hjälp av ett starkt lösenord eller en biometrisk identifiering och därefter kommer åt samtliga av sina sparade lösenord. Lösenorden kan lagras i lokalt eller i molnet beroende på hur lösenordshanteraren fungerar.

2.1.3 Tvåfaktorsautentisering

Tvåfaktorsautentisering är en teknik som låter en användare autentisera sig genom att inte bara kunna sitt lösenord utan även uppvisa ett ägande av en enhet såsom en telefon eller en USB-sticka (Jarecki et al., 2018, s.432). Det betyder att man förutom att ha tillgång till lösenordet även måste kunna styrka ägandet av exempelvis en telefon eller liknande för att få logga in och kan ske genom att man får ett sms till sin mobil (Jarecki et al., 2018, s.432) som sedan skrivs in efter man angett lösenordet. Det kan även röra sig om exempelvis en pin-kod som genereras från en app såsom Google Authenticator (Jarecki et al., 2018, s.432) eller Duo (Abbott och Patil 2020, s.1) som du har installerad på din telefon. Tvåfaktorsautentisering är alltså som det låter, två faktorer man behöver för att autentisera sig.

Tvåfaktorsautentisering ingår i begreppet multifaktorautentisering som innebär att man behöver uppvisa något man kan, något man har och något man kan (Abbott och Patil 2020, s.1). Exempel på detta är ett lösenord man lärt sig utantill, kanske en dator eller en enhet man har fysisk tillgång till och något man är, i form av en biometrisk faktor såsom ett fingeravtryck. Tvåfaktorsautentisering lyckas om man använder sig av två av dessa tre faktorer i inloggningsprocessen (Abbot och Patil, 2020, s.1).

Definitionen av tvåfaktorsautentisering är således en metod eller teknik för att uppnå extra säkerhet vid inloggning till olika system. Genom att kombinera sitt lösenord med exempelvis en inläsning av ett fingeravtryck eller en extra kod som genereras från en app eller liknande krävs två steg för att logga in i stället för ett som det hade varit om man bara använt sig av ett lösenord. Detta bidrar till en ytterligare dimension av lösenordssäkerhet då det inte

bara räcker att hacka ett lösenord utan du behöver också fysisk tillgång till något av de tidigare nämnda sakerna vilket ofta inte är möjligt för den som hackar.

2.2 Tidigare forskning om lösenordshantering

Följande avsnitt behandlar tidigare forskning kring lösenordshantering och två olika studier presenteras där resultaten är av relevans för en jämförelse med den här studiens resultat.

2.2.1 Införande av ny lösenordspolicy på Carnegie Mellon University

Shay et al., (2010) genomförde en studie på Carnegie Mellon University när universitetet beslutat att införa en förändring i sin lösenordspolicy. Denna policy tvingade användarna att ändra sina lösenord och det blev en chans för författarna att undersöka attityder och beteenden kring användande och skapande av olika lösenord. Studien genomfördes som en enkätundersökning med 470 deltagare där författarna samlade in data om användarnas beteenden och vanor kring skapandet och användandet av lösenord. Vidare ville de även undersöka användarnas åsikter om den nya skärpta policyn. Detta resulterade i en bild av att deltagarna kände sig säkrare efter lösenordsbytet trots att de var något irriterade över att behöva skapa ett komplext lösenord. Enkätundersökningen resulterade i ett antal upptäckter som är relevanta i den här studien. De kom bland annat fram till att 80% av deltagarna baserade sitt nya lösenord på ett namn eller ett vanligt ord, ibland kombinerat med specialtecken före och efter, trots att policyn var tydlig om att inte använda sig av så kallade “dictionary words”. Vidare visade studien att deltagarna tenderade att modifiera gamla lösenord för att skapa nya. Ungefär 50% av deltagarna valde att modifiera sitt gamla lösenord istället för att skapa ett helt nytt. Runt 25% av deltagarna angav också att de hade delat med sig av sitt gamla lösenord till minst en person. När det handlar om att återanvända lösenord angav 75% av användarna att de återanvänder lösenord. Sammanfattningsvis visar studien på ett antal intressanta punkter när det gäller lösenordssäkerhet och hanteringen av lösenord och på attityder kring detta.

2.2.2 Undersökning av vanor kring skapande och användande av lösenord på Southern Methodist University

Brown et al., (2004) genomförde en enkätundersökning på Souther Methodist University i USA för att ta reda på vanor kring skapandet och användandet av lösenord. Enkätundersökningen fylldes i av 218 studenter och resulterade i ett antal slutsatser. Deltagarna hade 8,18 lösenord i snitt. Över 90% av deltagarna använde information om sig själva som bas för att konstruera sina lösenord. 75% av deltagarna använde namnet på en sak, plats eller person för något eller flera av sina lösenord. Studien visade vidare på ett antal mönster inom återanvändande av lösenord. Endast 7,1% av deltagarna använde var och ett av sina lösenord till endast ett ställe. Hela 37,4% duplicerade endast ett lösenord på flera ställen. När det handlade om hur deltagarna hanterade sina lösenord angav över hälften, 54,1% att de har skrivit ner sina lösenord någonstans.

2.3 Tidigare forskning om äldres acceptans för tekniska hjälpmedel inom lösenordshantering

Ray et al., (2021) har i sin studie undersökt huruvida äldre är eller inte är motiverade att använda lösenordshanterare. Studien är kvalitativ men en skala presenteras i metoden för hur studien kan tolkas på ett kvantitativt sätt. Författarna har utfört 26 semi-strukturerade intervjuer med personer över 60 år, vad de i studien kallar för äldre vuxna. En studie som på grund av urvalets ålder blir högst relevant att ta med inför den här undersökningen. Av deltagarna som var med i studien var det 10 st., alltså cirka 38% som inte använde sig av en lösenordshanterare. Medelåldern var för dessa 70,9 år. 9 st., och alltså cirka 35% använde en inbyggd lösenordshanterare och medelåldern för dessa var 70,6 år. 7 st. och 27% använde en egenhändigt installerad lösenordshanterare och medelåldern för dessa var 69,4 år.

Studien resulterade i ett antal intressanta observationer varav en var att över hälften och de flesta (55-75%) av deltagarna var medvetna om starka lösenord och att man bör konstruera dem med bokstäver, nummer och/eller specialtecken. Hur deltagarna gjorde för att konstruera sina lösenord skilde sig mellan de som använde och inte använde lösenordshanterare. De som inte använde lösenordshanterare tenderade att konstruera lösenorden efter egna fraser och ord med personligt innehåll. De som använde sig av inbyggda lösenordshanterare valde ofta att själva skapa mer komplexa lösenord och de som själva installerat lösenordshanterare använde sig av lösenordshanterarens funktion för att generera slumpmässiga lösenord.

2.4 CIA-triaden

CIA-triaden är ett vanligt begrepp inom informationssäkerhet sen många år tillbaka (Samonas och Coss, 2014, s.21) och står för “confidentiality”, “integrity” och “availability”. Begreppet CIA-triaden hänvisar i grund och botten till de grundläggande komponenter som bör finnas för säkerhetskontroller i informationssystem (Samonas och Coss, 2014, s.21-22) och kan således användas som en grund till att veta hur man skyddar information. Begreppet har en lång historia och har byggts på definierats om i olika omgångar till det det står för idag (Samonas och Coss, 2014). I den här studien används begreppet CIA-triaden som ett ramverk i utformandet av frågorna då lösenordshantering i allra högsta grad innefattas i begreppet informationssäkerhet.

Beståndsdelarna i CIA-triaden går ibland lite in i varandra men huvudsakligen står de olika begreppen för det här:

- **Confidentiality (konfidentialitet)**
    - Informationen ska bara vara tillgänglig för dem som den är tänkt att användas av (van der Ham, 2021, s.1). Inom lösenordssäkerhet kan det alltså tolkas som att ingen annan än den som ska använda lösenordet bör ha tillgång till det.
- **Integrity (integritet)**
    - Informationen ska bevisligen inte ha kunnat ändras eller modifieras av någon (van der Ham, 2021, s.1). Inom lösenordssäkerhet kan det innebära att lösenorden exempelvis ska lagras på en säker plats där ingen kan komma åt dem och ändra dem.
- **Availability (tillgänglighet)**
    - Informationen ska vara åtkomlig för den som är tänkt att använda den (van der Ham, 2021, s.1). Detta kan inom lösenordssäkerhet innebära att man som innehavare av ett lösenord exempelvis kanske förvarar sina lösenord på en plats där man vet att man har tillgång till dem när helst man behöver dem.

3 Metod

Följande kapitel behandlar inledningsvis den övergripande forskningsstrategin som har valts för uppsatsen samt ett resonemang kring uppsatsens forskningsparadigm. Vidare behandlas metodiken för datainsamling med resonemang kring utformning av vald metod samt vilket urval och vilken urvalsmetod som använts. Slutligen beskriver kapitlet vilken metod för dataanalys och följaktligen vilka statistiska metoder som använts.

3.1 Övergripande forskningsstrategi och forskningsparadigm

Forskningsstrategin som antagits inför studien är en surveyundersökning av kvantitativ karaktär. En surveyundersökning möjliggör enligt Oates (2006, s.93) att få in samma typ av data från en större grupp av människor, och att detta då sker på ett standardiserat och systematiskt sätt. I den här studien har datan samlats in med hjälp av en enkätundersökning där målet har varit att nå minst 50 personer. När man sedan fått in datan man efterfrågar kan man analysera den och se mönster i den för att kunna applicera slutsatserna på en större grupp människor än de man faktiskt undersökt, detta kallas för att generalisera (Oates, 2006 s.93). Ambitionen har därför varit att få in ett större antal svar för att kunna generalisera kring de slutsatser som kan dras från dem. Diskussioner kan dock föras kring hur generaliserbar datan blir beroende på hur stort och brett urval man får in och den diskussionen förs nedan i avsnittet för urvalsmetod.

Eftersom surveyundersökningar syftar till att få fram mönster och en möjlighet att generalisera associeras de ofta inom forskningsparadigmet positivism där målet är just detta (Oates, 2006, s.93). Därav faller även den här studien inom forskningsparadigmet positivism då det funnits en önskan om att kunna dra generaliserande slutsatser kring den övergripande medvetenheten hos både yngre och äldre när det handlar om lösenordssäkerhet- och hantering. Syftet med studien har alltså inte varit att kvalitativt undersöka människors beteende gällande dessa frågor utan snarare att endast se till medvetenheten kring detta med hjälp av en kvantitativ och ganska ytlig studie. Målet har inte på något sätt varit att förstår varför och hur utan bara om. Inom positivismen är det vanligt att använda sig av statistiska metoder för att analysera den insamlade datan (Oates, 2006, s.286) och det har således gjorts även i den här studien.

3.2 Datainsamlingsmetodik

I det här avsnittet presenteras arbetet med enkäten utförligt. Enkätutformningen, formuleringen av frågorna och pilotstudien behandlas. Vidare presenteras också studiens urval och urvalsmetod.

3.2.1 Enkätutformning

Studien har som nämnts ovan alltså genomförts som en enkätundersökning och detta genom Google Forms. Målet med undersökningen och därmed även enkäten har som sagt varit att undersöka deltagarnas inställning och attityd kring lösenordssäkerhet- och hantering. Inte specifikt varför eller hur de använder sig av lösenord utan bara om de gör på ett visst sätt eller inte. Enkäten har därför som syfte att skrapa på ytan vilket gör att enkätens omfattning inte är alltför stor. En alltför omfattande enkät kan även göra att deltagarna lämnar och undviker att slutföra undersökningen vilket har velats undvika i den här studien.

När man skriver en enkät är det inte bara att skriva ner ett antal frågor på ett papper och tro att man ska få tillfredsställande svar, utan en enkät måste vara genomtänkt så att man får tag i giltig och pålitlig data (Oates, 2006, s.220). I arbetet med enkäten har detta varit viktigt och ett iterativt arbetssätt har därför antagits med både enkäten som helhet och frågorna i sig där frågorna bearbetats i olika omgångar. Det gäller även att på förhand veta hur man vill tolka datan man får in (Oates, 2006, s.220) och mycket tid har därför gått åt att säkerställa att detta ska vara möjligt för att öka studiens validitet.

Enkäten resulterade i 16 frågor där fråga 1-3 behandlar deltagarnas åldrar och vanor kring användandet av enheter och antal lösenord man anser sig använda per vecka. De tre inledande frågorna syftar till att ge en bild av de som deltar i enkäten och kommer inte att analyseras statistiskt. De övriga 13 frågorna handlar om deltagarnas medvetenhet och attityd till lösenordssäkerhet- och hantering och kommer analyseras statistiskt.

3.2.2 Frågeformulering

För att säkerställa att frågorna i enkäten håller en hög standard har ramverket CIA som behandlar informationssäkerhet använts som underlag. 12 av de 16 frågorna har skrivits med ramverket i åtanke och har därför delats in i de tre kategorier som CIA behandlar; *confidentiality*, *integrity* och *availability* (van der Ham, 2021, s.1). Dessa kategorier har inte presenterats på något sätt för deltagarna utan använts som en resurs i utformandet av frågorna. Tabellerna nedan visar vilka frågor som hamnat i vilken kategori och varför.

Confidentiality

Fråga:	**Motivering:**
5. Har du medvetet gett någon i din närhet tillgång till ett/flera av dina lösenord?	Frågan rör huruvida informationen endast är tillgänglig för den som är tänkt att använda den och kopplas därmed till confidentiality.
6. Har du lämnat ut ett/flera av dina lösenord till någon som kontaktade dig från en myndighet, bank, företag eller liknande vid något tillfälle?	Frågan rör huruvida informationen endast är tillgänglig för den som är tänkt att använda den och kopplas därmed till confidentiality.
14. Vet du vad tvåfaktorsautentisering är?	Frågan rör huruvida endast den som är tänkt att genomföra inloggningen har möjlighet att göra det och kopplas därmed till confidentiality.
15. Händer det att du använder dig av tvåfaktorsautentisering när det finns tillgängligt?	Frågan rör huruvida endast den som är tänkt att genomföra inloggningen har möjlighet att göra det och kopplas därmed till confidentiality.

Figur 1 - Tabell över frågornas indelning inom confidentiality.

Integrity

Fråga:	**Motivering:**
7. Är du extra mån om att välja ett säkert lösenord till ditt mejlkonto?	Frågan kan kopplas till integrity då ett dåligt lösenord på mejlen kan göra att någon som hackar det får möjlighet att ändra det lösenordet och andra lösenord som är kopplade till mejlen.
8. Händer det att du återanvänder samma lösenord på flera ställen?	Frågan kan kopplas till integrity då återanvändning av lösenord också kan göra att en hacker som får tag i

	ett lösenord sedan kan använda sig av det för att ta över/ändra användarens andra lösenord.
9. Har du som vana att ta med någon form av personlig information i dina lösenord, såsom din adress, namnet på ditt husdjur, ett smeknamn eller liknande?	Frågan kan kopplas till integrity då någon lätt kan lista ut ditt lösenord om det är kopplat till dig som person och ta över dina konton/ändra lösenorden.
10. Förvarar du något av eller alla dina lösenord på ett ställe där andra kan komma åt och se dem/ändra dem?	Frågan kopplas till integrity då den handlar om att någon kan komma åt och se eller ändra en användares lösenord.

Figur 2 - Tabell över frågornas indelning inom integrity.

Availability

Fråga:	**Motivering:**
11. Hur går du tillväga när du skapar nya lösenord?	Frågan kopplas till availability då den handlar om att den som skapar lösenorden ska ha åtkomst till dem. Frågans svarsalternativ rör lösenordshanterare som ett "program som skapar lösenordet åt användaren" och därför hamnade frågan i availability.
12. Använder du ett enligt dig strukturerat sätt för att hålla ordning på dina lösenord?	Frågan kopplas till availability då den handlar om att den som skapar lösenorden ska kunna få åtkomst till dem när det krävs.
13. Vet du vad en lösenordshanterare är?	Frågan kopplas till availability då den handlar om att den som skapar lösenorden ska kunna få åtkomst till dem när det krävs.
16. Skulle du vara intresserad av att börja använda en lösenordshanterare*? *En lösenordshanterare är ett program som lagrar alla dina lösenord och som du får åtkomst till genom att bara minnas ett starkt lösenord.	Frågan kopplas till availability då den handlar om att den som skapar lösenorden ska kunna få åtkomst till dem när det krävs.

Figur 3 - Tabell över frågornas indelning inom availability.

De övriga fyra frågorna har som sagt dels varit en öppen fråga om deltagarens ålder samt tre frågor kring deltagarens vanor kring lösenordsanvändning och självupplevd medvetenhet inom ämnet lösenordssäkerhet.

Det finns flera viktiga aspekter att tänka på när man utformar frågor till en enkät, bland annat bör frågorna vara utformat på ett objektivt sätt (Oates, 2006, s.222). En fråga bör inte leda deltagarna fram till ett givet svar (Oates, 2006, s.222) utan deltagarna ska genom frågans utformning få chansen att tänka och svara själva. Målet i utformningen av frågorna till enkäten har därför varit att eventuella förutfattade meningar hos författaren och vad denne själv anser är rätt eller inte i en fråga inte ska synas igenom så att deltagaren kan uppfatta ett svar som mer rätt än ett annat. Då det inom lösenordssäkerhet och hanteringen av lösenord kanske ibland finns ett svar som är mer rätt än ett annat har objektivitet och att undvika ledande frågor varit extra viktigt under arbetet med frågorna.

Frågorna i en enkät bör också vara korta, relevanta och specifika (Oates, 2006, s.221-222.) och därför är frågorna i den här enkäten utformade att innehålla så mycket information i en så kort fråga som möjligt. En fråga som blir alltför lång riskerar att bli svårtolkad och tappar därmed eventuellt också sin precision. En lång fråga kanske oftare tenderar att innehålla två frågor i en och det vill man undvika för att få precisa frågor (Oates, 2006, s.222). För långa och krångliga frågor kan också få deltagarna att avbryta enkäten i

förtid. Då den här studien hänger på att rekrytera deltagare som sedan slutför enkäten har just dessa kriterier varit extra viktiga i arbetet med utformandet av frågorna. Den slutgiltiga längden på enkäten har också velat hållas nere för att öka chansen att deltagarna slutför den och därför resulterade enkäten i totalt 16 frågor.

3.2.3 Pilotstudie

Frågorna har efter utformandet testats av några personer för att fånga upp eventuella svagheter och förbättra den ytterligare innan det slutgiltiga utskicket. De tre personerna som analyserat och testat enkäten är en chef inom it-branschen med stort intresse för it-säkerhet, en ekonomistudent som skriver motsvarande uppsats i ekonomi just nu samt en person med examen i politisk kandidat som själv nyligen genomförde en enkätundersökning.
Förslag och feedback från dessa tre har förbättrat enkäten väsentligt och för att ta ett exempel på ett förslag till förbättring som kom från ekonomistudenten var att frågan som lyder *"Hur många tjänster använder du regelbundet som kräver inloggning med hjälp av lösenord?"* var för vag och att jag skulle ändra regelbundet till en vald tidsram. Därför ändrades frågan till *"Hur många tjänster använder du per vecka som kräver inloggning med hjälp av lösenord?"*.

3.2.4 Urval

Den målgrupp som undersökts har avgränsats till vuxen ålder, vilket inkluderar deltagare från 18 år och uppåt. Detta på grund av att deltagarna själva bör kunna besluta om att delta i studien och därför behöver vara myndiga. För att underlätta inför kommande dataanalys har undersökningen skett endast på svenska och deltagarna har därför behövt vara svensktalande. Ingen avgränsning har gjorts kring utbildning, arbete eller liknande utan fokuset har legat på att jämföra användandet och acceptansen utifrån ålder och inga andra faktorer.

Ett bra riktmärke för små studier där författaren kanske genomför sin första undersökning är att få in minst 30 svar. Ett urval på färre än 30 personer det svårt att analysera datan statistiskt och resultatet blir också lite opålitligt. (Oates, 2006, s.100)
Målet var därför inför enkätutskicket att försöka nå minst 50 personer, för att ha lite marginal mot de 30 som Oates (2006, s.100) ser som minimum. Summan hamnade slutligen på 66 svar vilket får ses som tillräckligt i sammanhanget. En god spridning mellan åldrarna uppnåddes också vilket på förhand även sågs som viktigt baserat på uppsatsens syfte. Medelåldern på deltagarna landade på 47,95 år.

3.2.5 Urvalsmetod

När man satt ramarna för vilka som ska delta i studien, behöver man bestämma sig för en urvalsmetod (Oates, 2006, s.96). Urvalsmetoden för den här studien har varit en typ av "snöbollsurval" som faller under kategorin "icke-probabilitetsurval". Snöbollsurval möjliggör att forskaren själv kontaktar en person som stämmer in på urvalskriterierna för att sedan få rekommendationer av den om fler personer som skulle vara intresserade av att delta i undersökningen (Oates, 2006, s.98). En av de viktigaste parametrarna inför enkätundersökningen var att få en bra spridning i ålder på de som deltog. Därför skickades länken till enkäten först ut till ett tiotal personer i spridda åldrar i författarens närhet. När de fyllt i enkäten ombads de skicka vidare länken till människor i sin närhet och åldersgrupp. Detta har gjort att en bra spridning mellan åldrarna uppnåtts.

Diskussioner kan dock föras kring hur generaliserbart detta tillvägagångssätt blir då många som fyllt i enkäten troligtvis befinner sig i liknande nätverk och samhällsgrupper. Detta nämner också Oates (2006, s.96) i sitt resonemang kring icke-probabilitetsurval. Hon

menar att dessa typer av urval ger ett svagt underlag för generaliseringar inom populationen men skriver också att det kan vara godtagbart när brist på tid finns eller att forskaren själv inte anser att det är nödvändigt med ett representativt urval (Oates, 2006, s.97). I den här studien har bristen på tid setts som ett skäl till att ändå använda sig av ett sådant urval. Däremot finns en medvetenhet hos författaren att studiens generaliserbarhet och reliabilitet påverkas och att det är inte är helt säkert att studien skulle få samma resultat om den gjordes om.

3.3 Metod för dataanalys

När enkäten varit ute i två veckor avslutades insamlingen av svar och analysen kunde påbörjas. Svaren sammanställdes efter avslutad insamling i Excel och analyserades senare främst i programmet SPSS (IBM, 2022) och till viss del med hjälp av VassarStats (Lowry, 2022). Datan har analyserats statistiskt med hjälp av Chi Square-metoden för att undersöka sambandet mellan ålder och medvetenhet kring lösenordssäkerhet och hur deltagarna hanterar sina lösenord. Chi Square-metoden fungerar inte tillförlitligt när mer än 20% av cellerna har färre än 5 observationer i förväntat antal eller någon cell har 0 i värde (Yates et al., 1999). Därför har de frågor som inte nått upp till detta istället analyserats med Fisher's Exact Test som fungerar bättre vid ett mindre urval (Gaddis & Gaddis, 1990, s.1055). Som tidigare nämnt har inte fråga 1-3 analyserats statistiskt då de har som syfte att klargöra vilka som deltar i undersökningen. Fråga 4-16 har däremot analyserats statistiskt.

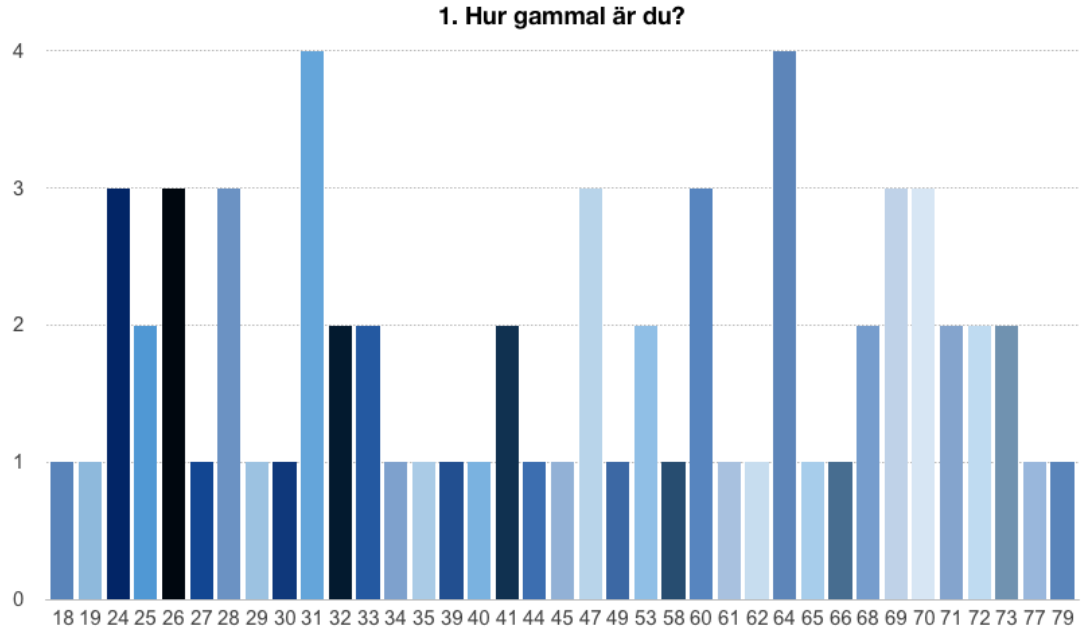
Chi Square-metoden och Fisher's Exact Test fungerar båda med nominell data (Gaddis & Gaddis, 1990, s.1054) vilket är den typen av data som använts i enkätundersökningen för de frågor som ska analyseras statistiskt. Samtliga av dessa frågor har därför gått att analysera på ett bra sätt med dessa metoder. Båda dessa metoder är mäter huruvida det finns en statistisk signifikans mellan två oberoende grupper eller inte (Gaddis & Gaddis, 1990, s.1054-1055) och därför har deltagarna delats in i två olika åldersgrupper efter att enkäten var avslutad. Planen innan enkätutskicket var att inför analysen dela upp deltagarna i två grupper varav en med deltagare under 65 år och en med deltagare som var 65 år och äldre. Då det rådde en viss ovisshet kring hur spridningen av svar skulle te sig togs det beslutet helt definitivt när svaren väl kommit in och det visade sig vara möjligt med den uppdelningen. Signifikanstester visar vid uträkningen ett signifikansvärde som hjälper till att avgöra om det finns en statistiskt bevisad skillnad mellan grupperna eller inte (Oates, 2006, s.259). Detta signifikansvärde brukar som standard vara 0,05 (Oates, 2006, s.261) och används därför som alfavärde i även den här studien.

4 Resultat

Följande kapitel behandlar resultatet för enkätundersökningen. Deskriptiv statistik presenteras för alla frågor som ingick i undersökningen.

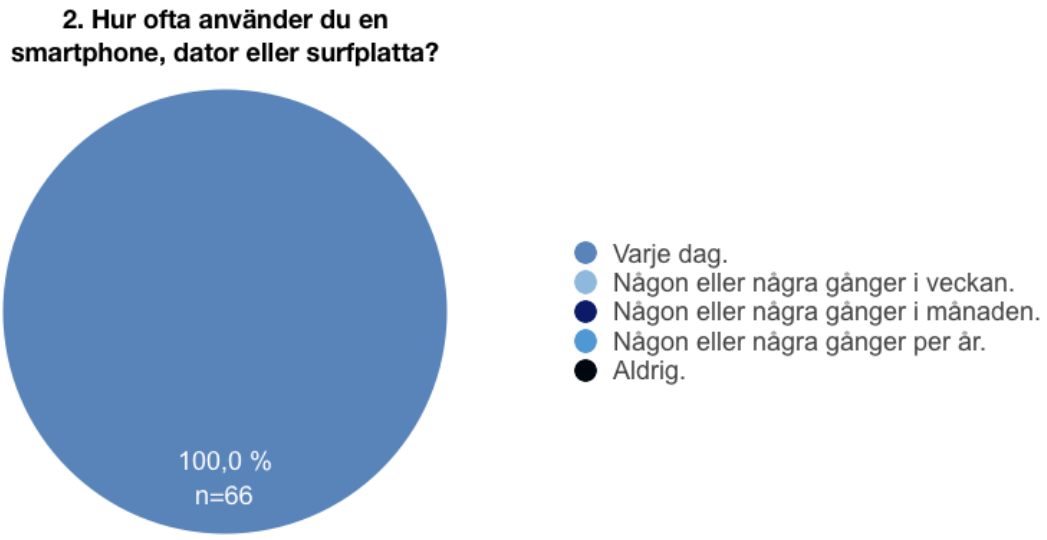
4.1 Deltagarna i studien

Följande diagram behandlar information om deltagarna i studien. Enkäten inleddes med tre frågor varav en visar deltagarnas ålder och de andra två deltagarnas användning av enheter och tjänster som kräver hantering av lösenord.



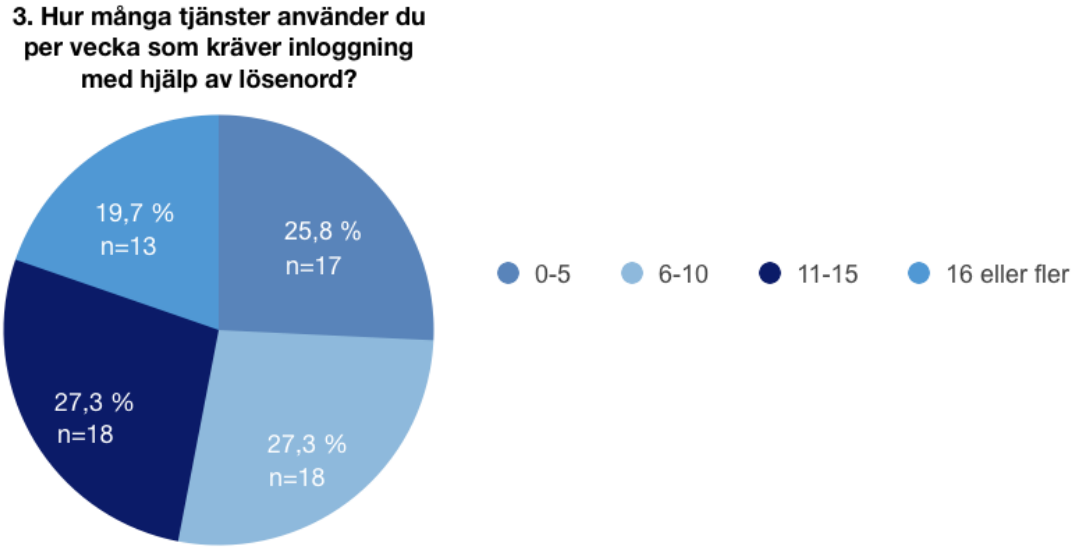
Figur 4 - Fördelning av deltagarnas åldrar.

Figuren ovan är ett histogram som visar åldersfördelningen på de som deltagit i studien. Medelåldern på deltagarna är 47,95 år. Drygt 27% av deltagarna i enkäten är 65 år och äldre.



Figur 5 - Fördelning av hur ofta deltagarna använder en smartphone, dator eller surfplatta.

Figuren ovan visar hur ofta deltagarna i studien använder sig av antingen en smartphone, dator eller surfplatta. 100% (n=66) av deltagarna använder någon av dessa enheter varje dag.



Figur 6 - Fördelning över hur många tjänster deltagarna använder per vecka som kräver inloggning med lösenord.

Figuren ovan visar antal tjänster som deltagarna använder per vecka som kräver inloggning med hjälp av lösenord. 25,8% (n=17) använder 0-5 tjänster, 27,3% (n=18) använder 6-10 respektive 11-15 tjänster medan 19,7% (n=13) använder 16 eller fler tjänster varje vecka som kräver inloggning med lösenord.

4.2 Deltagarnas egna medvetenhet

4. Anser du själv att du har en medvetenhet kring vad som gör ett lösenord säkert?	Ja	Till viss del.	Nej
	50 %	45,5 %	4,5 %

Figur 7 - Fördelning av svaren på frågan om deltagaren själv upplever sig ha en medvetenhet kring vad som gör ett lösenord säkert.

Figuren ovan visar på deltagarnas egen medvetenhet när det handlar om vad som gör ett lösenord säkert. 50% (n=33) har svarat att de har en medvetenhet kring detta, 45,5% (n=30) har svarat att de har en viss medvetenhet och 4,5% (n=3) har svarat att de inte har en medvetenhet kring detta.

4.3 Confidentiality

Följande avsnitt behandlar ämnet confidentiality och således frågor som rör huruvida endast den som ska ha tillgång till lösenorden eller informationen har det. Frågor som rör huruvida deltagaren har lämnat ut sitt lösenord till någon annan och hur denne ser på tvåfaktorsautentisering behandlas.

5. Har du medvetet gett någon i din närhet tillgång till ett/flera av dina lösenord?	Ja	Nej	
	77,3 %	22,7 %	
6. Har du lämnat ut ett/flera av dina lösenord till någon som kontaktade dig från en myndighet, bank, företag eller liknande vid något tillfälle?	Ja	Nej	
	3 %	97 %	
14. Vet du vad tvåfaktorsautentisering är?	Ja, jag är väl medveten om vad det är.	Ja, men bara till viss del.	Nej
	45,5 %	24,2 %	30,3 %
15. Händer det att du använder dig av tvåfaktorsautentisering?	Ja	Nej	Jag vet inte vad tvåfaktorsauten tisering är.
	51,5 %	19,7 %	28,8 %

Figur 8 - Fördelning av svaren på frågorna 5, 6, 14 och 15.

På frågan om huruvida deltagaren har gett någon i sin närhet tillgång till ett eller flera av sina lösenord är det 77,3% (n=51) som har svarat ja och 22,7% (n=15) som har svarat nej. På frågan om huruvida deltagaren medvetet har lämnat ut ett eller flera lösenord till någon som kontaktat denne från en bank, myndighet, företag eller liknande vid något tillfälle är det endast 3% (n=2) som svarat ja och 97% (n=64) som svarat nej. När det gäller huruvida deltagarna är medvetna om tvåfaktorsautentisering eller inte har 45,5% (n=30) svarat att de är väl medvetna om vad det är. 24,2% (n=16) har en viss medvetenhet kring tvåfaktorsautentisering medan 30,3% (n=20) inte vet vad det är. Angående deltagarnas inställning till att använda sig av tvåfaktorsautentisering så svarade ungefär hälften, alltså 51,5% (n=34) att det händer att de använder sig av tvåfaktorsautentisering när det finns tillgängligt. 19,7% (n=13) har svarat att de inte gör det medan 28,8% (n=19) har svarat att de inte vet vad tvåfaktorsautentisering är.

4.4 Integrity

Följande avsnitt behandlar ämnet integrity och således frågor som rör huruvida lösenorden hindras från att förändras eller modifieras av någon annan än den som har behörighet att göra det. Frågor som handlar om huruvida deltagaren tenderar att återanvända lösenord och hur denne förvarar dem är exempel på frågor som ingår.

7. Är du extra mån om att välja ett säkert lösenord till ditt mejlkonto?	Ja	Nej	
	65,2 %	34,8 %	
8. Händer det att du använder dig av samma lösenord på flera ställen?	Ja	Nej	
	86,4 %	13,6 %	
9. Har du som vana att ta med någon form av personlig information i dina lösenord, såsom din adress, namnet på ditt husdjur, ett smeknamn eller liknande?	Ja	Nej	
	34,8 %	65,2 %	
10. Förvarar du något av eller alla dina lösenord på ett ställe där andra kan komma åt och se dem/ändra dem?	Ja	Nej	Vet inte.
	19,7 %	75,8 %	4,5 %

Figur 9 - Fördelning av svaren på frågorna 7, 8, 9 och 10.

På frågan huruvida deltagaren är extra mån om att välja ett säkert lösenord till sitt mejlkonto är det 65,2% (n=43) och därmed en majoritet som svarat ja, 34,8% (n=23) har svarat nej. När det handlar om återanvändande av samma lösenord på flera ställen är det 86,4% (n=57) som svarat att det händer att de gör detta. 13,6% (n=9) har svarat nej och att det alltså inte händer

att de återanvänder sig av lösenord. På frågan huruvida deltagaren har som vana att ta med någon form av personlig information i sina lösenord eller inte är det 34,8% (n=23) som svarat ja och 65,2% (n=43) som svarat nej. Tabellen visar också att när det gäller förvaringen av lösenord är det 19,7% (n=13) som förvarar något eller alla sina lösenord på ett ställe där andra kan komma åt dem. 75% (n=50) har svarat nej och därmed att de inte förvarar lösenorden på ett ställe där andra kan komma åt dem. 4,5% (n=3) har svarat att de inte vet om de gör det eller inte.

4.5 Availability

Följande avsnitt behandlar ämnet availability och således frågor som rör huruvida användaren har tillgång till lösenorden närhelst denne behöver det. Frågor som rör huruvida deltagaren använder sig av ett strukturerat sätt för att hålla ordning på sina lösenord och frågor om lösenordshanterare är exempel på det som ingår i avsnittet.

11. Hur går du tillväga när du skapar nya lösenord?	Jag hittar själv på dem med hjälp av ord jag lätt kommer ihåg.	Jag slumpar fram dem själv eller med hjälp av ett program.	Annat
	80,3 %	7,6 %	12,1 %
12. Använder du ett enligt dig strukturerat sätt för att hålla ordning på dina lösenord?	Ja	Nej	
	66,7 %	33,3 %	
13. Vet du vad en lösenordshanterare är?	Ja, jag är väl medveten om vad det är.	Ja, men bara till viss del.	Nej
	31,8 %	34,8 %	33,3 %
16. Skulle du vara intresserad av att börja använda en lösenordshanterare*? *En lösenordshanterare är ett program som lagrar alla dina lösenord och som du får åtkomst till genom att bara minnas ett starkt lösenord.	Ja	Nej	Jag använder mig redan av en lösenordshanterare.
	48,5 %	33,3 %	18,2 %

Figur 10 - Fördelningen av svaren på frågorna 11, 12, 13 och 16.

Tabellen ovan visar att 7,6% (n=5) av deltagarna slumpar fram sina lösenord själva eller med hjälp av ett program. 80,3% (n=53) hittar själva på dem med hjälp av ord de lätt kommer ihåg. 12,1% (n=8) använder sig av ett annat sätt att skapa nya lösenord. På frågan huruvida deltagaren använder sig av ett strukturerat sätt för att hålla ordning på sina lösenord är det 66,7% (n=44) som svarat ja och 33,3% (n=22) som svarat nej. När det handlar om hur medvetna deltagarna är kring lösenordshanterare och vad det är är det 31,8% (n=21) som är väl medvetna om vad det är. 34,8% (n=23) har en viss medvetenhet kring vad en

lösenordshanterare är medan 33,3% (n=22) inte har det. Angående deltagarnas intresse för att börja använda en lösenordshanterare är det 48,5% (n=32) som svarat ja och därmed är intresserade av att börja göra det. 33,3% (n=22) har svarat nej och är således inte intresserade av att börja använda en lösenordshanterare. 18,2% (n=12) har uppgett att de redan använder sig av en lösenordshanterare.

5 Analys

I följande kapitel presenteras resultatet från den statistiska analysen som skett med Chi Square-metoden och Fisher's Exact Test. Samtliga av de fullständiga uträkningarna hittas bland bilagorna och endast de där resultatet visar på statistisk signifikans finns med i detta avsnitt. Alfavärdet som resultaten jämförts med är 0,05 och detta betyder alltså att om p-värdet är lägre än 0,05 visar resultatet på statistisk signifikans.

5.1 Deltagarnas egen medvetenhet

Fråga:	Test:	P-värde:	Statistisk signifikans:
4. Anser du själv att du har en medvetenhet kring vad som gör ett lösenord säkert?	Fisher's Exact Test	0,113	Nej

Figur 11 - Sammanfattning av den statistiska analysen av fråga 4.

Resultatet för fråga 4 visar inte på statistisk signifikans mellan grupperna då p-värdet inte är mindre än 0,05. De flesta i de båda åldersgrupperna svarade att de antingen har en medvetenhet i frågan eller att de har en viss medvetenhet. Det var väldigt få personer som svarade att de inte har det, bara 4,5% av deltagarna. Detta tyder på att de flesta som genomförde undersökningen tycker sig vara medvetna kring vad som gör ett lösenord säkert. Det är ingen garanti för att deltagarna faktiskt är insatta och medvetna kring vad som gör ett lösenord säkert men det kan vara intressant att se hur många som faktiskt upplever sig som medvetna.

5.2 Confidentiality

Fråga:	Test:	P-värde:	Statistisk signifikans:
5. Har du medvetet gett någon i din närhet tillgång till ett/flera av dina lösenord?	Fisher's Exact Test	1	Nej
6. Har du lämnat ut ett/flera av dina lösenord till någon som kontaktade dig från en myndighet, bank, företag eller liknande vid något tillfälle?	Fisher's Exact Test	1	Nej
14. Vet du vad tvåfaktorsautentisering är?	Chi Square	<0,001	Ja
15. Händer det att du använder dig av tvåfaktorsautentisering?	Chi Square	<0,001	Ja

Figur 12 - Sammanfattning av den statistiska analysen av fråga 5, 6, 14 och 15.

Den statistiska analysen av fråga 5 och 6 visar inte på någon statistisk signifikans då p-värdet för de båda frågorna är 1. Som nämnt i resultatet är det endast 3% (n=2) som har angett att de lämnat ut lösenord till någon som kontaktat dem från en myndighet, bank, företag eller liknande vilket är ett glädjande resultat. Många av deltagarna verkar alltså ha uppfattat att man inte bör lämna ut lösenord till någon som kontaktar en och ber om ens lösenord.

Vet du vad tvåfaktorsautentisering är?

Ålder		Ja, jag är väl medveten om vad det är	Ja, men bara till viss del.	Nej	Total
65 år och äldre	Count	1	3	14	18
	Share	5,6 %	16,7 %	77,8 %	100 %
Under 65 år	Count	29	13	6	48
	Share	60,4 %	27,1 %	12,5 %	100 %
Total	Count	30	16	20	66
	Share	45,5 %	24,2 %	30,3 %	100 %

Figur 13 - Statistisk uträkning av fråga 14.

När det handlar om fråga 14 och huruvida man vet vad tvåfaktorsautentisering är visar resultatet på statistisk signifikans då p-värdet är mindre än 0,05. Det framgår i figur 13 att det i gruppen 65 år och äldre bara är 5,6% som är väl medveten om vad tvåfaktorsautentisering är och 16,7% som till viss del vet vad det är. Detta kan ställas i kontrast till hur gruppen som är under 65 år ser på det, där är motsvarande andelar 60,4% respektive 24,2%. 77,8% i gruppen 65 år och äldre vet inte vad det är medan endast 12,5% i gruppen under 65 år är ovetande om tvåfaktorsautentisering.

Händer det att du använder dig av tvåfaktorsautentisering när det finns tillgängligt?

Ålder		Ja	Nej	Jag vet inte vad tvåfaktorsautentisering är.	Total
65 år och äldre	Count	1	3	14	18
	Share	5,6 %	16,7 %	77,8 %	100 %
Under 65 år	Count	33	10	5	48
	Share	68,8 %	20,8 %	10,4 %	100 %
Total	Count	34	13	19	66
	Share	51,5 %	19,7 %	28,8 %	100 %

Figur 14 - Statistisk uträkning av fråga 15.

Fråga 15 visar på huruvida det händer att deltagaren använder sig av tvåfaktorsautentisering när det finns tillgängligt och även den här frågan visar på statistisk signifikans mellan de båda grupperna då p-värdet är mindre än 0,05. Tabellen ovan visar att det i åldersgruppen 65 år och äldre bara är 5,6% som ibland använder sig av tvåfaktorsautentisering när det finns tillgängligt. Detta kan ställas i kontrast till gruppen under 65 år där hela 68,8% ibland använder sig av tvåfaktorsautentisering när det finns tillgängligt.

5.3 Integrity

Fråga:	Test:	P-värde:	Statistisk signifikans:
7. Är du extra mån om att välja ett säkert lösenord till ditt mejlkonto?	Chi Square	0,874	Nej
8. Händer det att du använder dig av samma lösenord på flera ställen?	Fisher's Exact Test	0,7	Nej
9. Har du som vana att ta med någon form av personlig information i dina lösenord, såsom din adress, namnet på ditt husdjur, ett smeknamn eller liknande?	Chi Square	0,187	Nej
10. Förvarar du något av eller alla dina lösenord på ett ställe där andra kan komma åt och se dem/ändra dem?	Fisher's Exact Test	0,071	Nej

Figur 15 - Sammanfattning av den statistiska analysen av fråga 7, 8, 9 och 10.

Resultatet för fråga 7, 8, 9 och 10 visar inte på någon statistisk signifikans mellan åldersgrupperna då inga av dess p-värden är mindre än 0,05. Detta tyder då på att det inte finns någon skillnad mellan hur de som är 65 år och äldre och de som är yngre än 65 år ser på dessa frågor.

5.4 Availability

Fråga:	Test:	P-värde:	Statistisk signifikans:
11. Hur går du tillväga när du skapar nya lösenord?	Fisher's Exact Test	0,676	Nej
12. Använder du ett enligt dig strukturerat sätt för att hålla ordning på dina lösenord?	Chi Square	0,558	Nej
13. Vet du vad en lösenordshanterare är?	Chi Square	0,244	Nej
16. Skulle du vara intresserad av att börja använda en lösenordshanterare*? *En lösenordshanterare är ett program som lagrar alla dina lösenord och som du får åtkomst till genom att bara minnas ett starkt lösenord.	Chi Square	0,014	Ja

Figur 16 - Sammanfattning av den statistiska analysen av fråga 11, 12, 13 och 16.

Analysen av frågorna 11, 12 och 13 visar inte på någon statistisk signifikans mellan grupperna då ingen av p-värdena är mindre än 0,05.

Skulle du vara intresserad av att börja använda en lösenordshanterare*? *En lösenordshanterare är ett program som lagrar alla dina lösenord och som du får åtkomst till genom att bara minnas ett starkt lösenord.

Ålder		Ja	Nej	Jag använder mig redan av en lösenordshanterare.	Total
65 år och äldre	Count	5	11	2	18
	Share	27,8 %	61,1 %	11,1 %	100 %
Under 65 år	Count	27	11	10	48
	Share	56,3 %	22,9 %	20,8 %	100 %
Total	Count	32	22	12	66
	Share	48,5 %	33,3 %	18,2 %	100 %

Figur 17 - Statistisk uträkning av fråga 16.

Däremot visar analysen av fråga 14 på statistisk signifikans mellan grupperna då p-värdet är mindre än 0,05. I tabellen nedan framgår det att i åldersgruppen 65 år och äldre är det 61,1% som inte är intresserade av att använda en lösenordshanterare. Samma andel är 22,9% i gruppen för de som är under 65 år vilket tyder på att de i den yngre gruppen har ett större intresse för att börja använda en lösenordshanterare.

6 Avslut

Följande kapitel behandlar inledningsvis en diskussion kring den statistiska signifikans som påvisats och de exceptionella resultat som undersökningen visat. Vidare görs jämförelse mot tidigare forskning. Slutsatser dras och studiens generaliserbarhet diskuteras. Slutligen presenteras förslag på framtida forskning inom ämnet.

6.1 Diskussion

Följande avsnitt är uppdelat i två delar. Den första delen behandlar de frågor som påvisade en statistisk signifikans och vidare några frågor där resultatet inte är statistiskt signifikant men där det finns andra intressanta parametrar att diskutera. Den andra delen behandlar tidigare forskning i ämnet och jämförelser görs mot den tidigare forskningen med resultat från den här studien.

6.1.1 Statistisk signifikans och exceptionella resultat

Analysen visar tydligt att det finns en statistisk signifikans mellan de båda åldersgrupperna i 3 av 13 frågor. Det rör sig om följande frågor:

- Vet du vad tvåfaktorsautentisering är?
- Händer det att du använder dig av tvåfaktorsautentisering när det finns tillgängligt?
- Skulle du vara intresserad av att börja använda en lösenordshanterare?

När det handlar om första frågan och hur medvetna de båda grupperna är kring tvåfaktorsautentisering är resultatet tydligt. P-värdet är mindre än 0,001 och därmed även mindre än 0,05 och visar därmed på statistisk signifikans. Gruppen som är under 65 år är klart mer medvetna om vad tvåfaktorsautentisering är jämfört med de som är 65 år och över. Andra frågan handlar om huruvida deltagaren använder sig av tvåfaktorsautentisering när det finns tillgängligt. Även här visar det sig att den yngre gruppen, alltså de under 65 år är mer medvetna när det gäller tvåfaktorsautentisering. Den yngre gruppen är statistiskt sett mer benägna att använda sig av tvåfaktorsautentisering när det finns tillgängligt än den äldre åldersgruppen. P-värdet är likt den första frågan även här mindre än 0,001 och visar därmed på statistisk signifikans. Slutligen visar även frågan om huruvida deltagaren är intresserad av att börja använda en lösenordshanterare på en statistisk signifikans mellan grupperna. P-värdet är 0,014 och därmed mindre än 0,05 och visar att den yngre gruppen även i den här frågan visar mer intresse och medvetenhet kring lösenordshanterare än den äldre gruppen med deltagare som är 65 år och över.

För de övriga 10 statistiskt analyserade frågorna finns ingen statistisk signifikans och i de fallen kan därmed ingen slutsats dras kring skillnaden mellan gruppernas medvetenhet. Däremot visar vissa av de övriga frågorna i enkäten, inklusive de som inte analyserats statistiskt, på några andra intressanta slutsatser. På frågan som undersökte deltagarnas egna upplevda medvetenhet kring lösenordssäkerhet, "*Anser du själv att du har en medvetenhet kring vad som gör ett lösenord säkert?*", var det endast 4,5% som svarade nej. Detta bådar gott för att deltagarna själva är insatta i konceptet lösenordssäkerhet. Däremot är det som tidigare även nämnt i analysen ingen garanti för att deltagarna faktiskt är medvetna kring vad som är viktigt inom lösenordssäkerhet. När det handlar om frågan "*Hur ofta använder du en smartphone, dator eller surfplatta?*" kan det konstateras att 100% av deltagarna i enkäten har svarat varje dag. I den här studien verkar ålder således inte vara en avgörande faktor för användandet av den här typen av teknik. På frågan "*Har du lämnat ut ett/flera av dina*

lösenord till någon som kontaktade dig från en myndighet, bank, företag eller liknande vid något tillfälle?" var det 97% som svarade nej vilket givetvis är glädjande då det är viktigt att hålla sina lösenord privata och inte lämna ut dem till andra.

6.1.2 Jämförelse med tidigare forskning

Vidare har 86,4% har svarat ja på frågan "*Händer det att du återanvänder samma lösenord på flera ställen?*". Som tidigare nämnt i teorin är det enligt flera experter viktigt att inte återanvända samma lösenord på flera ställen då en hacker som kommer åt ett av lösenorden sedan kan ta sig in på flera andra ställen med samma lösenord (Bain et al., 2010 s.257) (Ives et al., 2004, s.76). Resultatet i den här studien kan jämföras med resultatet från den tidigare forskningen där det i undersökningen av Shay et al., (2010) också visade sig att många tenderade att återanvända lösenord. I den undersökningen uppgav 75% att de återanvände lösenord och det är ett snarlikt resultat jämfört med den här undersökningen där det var 86,4% som svarade att det händer att de återanvänder samma lösenord på flera ställen. Studien av Brown et al., (2004) visade också på ett antal mönster inom lösenordshantering där återanvändande var en del av dem. I deras undersökning kom det fram att endast 7,1% av deltagarna använde var och ett av sina lösenord till endast ett ställe. Detta innebär att 92,9% av deltagarna i deras undersökning återanvände lösenord till mer än ett ställe och är också snarlikt resultatet i den här studien. Det ska dock poängteras att studierna av Shay et al., (2010) och Brown et al., (2004) inte var begränsade till att undersöka just ålder hos deltagarna och därmed skiljer sig deras urval något från den här studiens urval. Trots detta är resultatet snarlikt vilket borde tala för att ålder inte spelar så stor roll när det handlar om beteendet kring återanvändning av lösenord.

På frågan "*Hur går du tillväga när du skapar nya lösenord?*" svarade 80,3% att de hittar på dem själv med hjälp av ord de lätt kommer ihåg. Detta är inte en bra strategi då man som nämnt i teorin helst ska undvika att använda ord från en ordbok (Bain et al., 2010 s.257) och istället använda sig av en kombination av alfanumeriska tecken och specialtecken (Ma et al., 2010, s.586). I jämförelse med tidigare forskning fanns det i både studien av Shay et al. (2010) och av Brown et al.:s, (2004) resultat kring hur deltagarna skapade nya lösenord. I studien av Shay et al., (2010) visade det sig att 80% av deltagarna baserade sitt nya lösenord på ett namn eller vanligt ord, ibland i kombination med specialtecken före och efter, trots att den nyinförda policyn var tydlig om att det inte skulle göras. Även i studien av Brown et al., (2004) visade det sig att 75% av deltagarna använde namnet på en sak, plats eller person för något eller flera av sina lösenord. Även dessa siffror är i samma spann som resultatet i den här studien och kan då också indikera att ålder inte är en avgörande faktor kring attityden och beteendet när man skapar nya lösenord. I studien av Ray et al., (2021) som specifikt undersökte äldres inställning och användande av lösenordshanterare kom det fram att de 38% som inte använde lösenordshanterare tenderade att konstruera lösenorden efter egna fraser och ord med personligt innehåll. De som använde sig av inbyggda lösenordshanterare valde ofta att själva skapa mer komplexa lösenord och de som själva installerat lösenordshanterare använde sig av lösenordshanterarens funktion för att generera slumpmässiga lösenord. Detta tyder på att de som använder lösenordshanterare kanske har en något högre grad av medvetande kring vad som är viktigt när man skapar nya lösenord.

Slutligen var det endast 11,1% i den här studien som i åldersgruppen 65 år och äldre uppgav att de använde sig av en lösenordshanterare. I studien av Ray et al., (2021) var det hela 62% som använde sig av en inbyggd eller egenhändigt installerad lösenordshanterare vilket var betydligt fler.

6.2 Slutsatser

Sammanfattningsvis visar både den här studien och tidigare studier på att det finns en del brister medvetandet kring lösenordssäkerhet och användandet av lösenord och tekniska hjälpmedel för dessa. I jämförelse med tidigare studier visar inte den här studien på något särskilt exceptionellt resultat när det handlar om skapandet av nya lösenord och återanvändandet av lösenord, däremot finns det en skillnad mot tidigare forskning i hur många äldre som använder sig av en lösenordshanterare.

Den statistiska analysen i den här studien visar också tydligt att det finns en signifikans mellan åldersgrupperna, specifikt i medvetandet kring tvåfaktorsautentisering och användandet av detta, men också i intresset för att använda sig av och användandet av lösenordshanterare. Den äldre gruppen med deltagare som är 65 år och äldre har bevisligen sämre medvetenhet kring dessa frågor.

Syftet med den här studien är att ta reda på om det finns skillnader i medvetenheten kring lösenordssäkerhet- och hantering mellan äldre och yngre och hur dessa skillnader i så fall ser ut. Det kan konstateras att det finns skillnader i detta. Dock inte i så stor utsträckning utan enligt den här studien endast kring intresset av att använda sig av lösenordshanterare och medvetandet kring och användandet av tvåfaktorsautentisering. I övrigt är det till synes ingen skillnad mellan åldrarna när det gäller medvetandet kring lösenord och en säker hantering av dessa.

6.3 Studiens generaliserbarhet

En diskussion kring detta fördes i avsnittet för urvalsmetod men tål att upprepas. Då studien genomfördes med snöbollsurval som urvalsmetod och att urvalet därmed inte är helt slumpmässigt kan göra att studiens generaliserbarhet påverkas. Detta då användningen av snöbollsurval tenderar att göra så att deltagarna är mer lika varandra än om de slumpmässigt valts ut då de kanske ofta befinner sig i samma typ av samhällsgrupp eller nätverk. Däremot motiverades detta typ av urval tydligt i metoden, och då främst på grund av den snäva tidsram som fanns för projektet. En medvetenhet kring att studien inte är helt generaliserbar finns ändå och risken finns att studiens resultat skulle komma att se annorlunda ut om den upprepades.

6.4 Förslag på framtida forskning

Då studien visar på brister när det gäller äldres intresse av att använda lösenordshanterare och medvetenhet kring tvåfaktorsautentisering och användandet av detta bör framtida forskning medverka till att detta förändras. Det är viktigt att forskningen kring äldre och lösenordssäkerhet fortsätter för att verka till att den här gruppen ska kunna ta del av allt som sker digitalt och känna sig säkra när de använder tjänster som kräver lösenord. Där är lösenordshanterare och tvåfaktorsautentisering en viktig del. I arbetet med uppsatsen har det visat sig att det inte finns så mycket forskning kring äldre och dessa frågor vilket visar på att det fortfarande är ett ganska outforskat ämne. En mer djupgående studie kring varför äldre har en sämre medvetenhet kring dessa frågor kan således vara aktuell.

Då urvalet av tidsbrist inte heller var helt slumpmässigt i den här studien kan även framtida studier med ett mer slumpmässigt urval göras för att se huruvida man får samma resultat eller inte.

7 Källförteckning

Abbott, J. Patil, S. (2020). “How mandatory second factor affects the authentication user experience” *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, p.1-13

Ahmed, E. DeLuca, B. Hirowski, E. Magee, C. Tang, I. Coppola, J.F. (2017). “Biometrics: Password replacement for elderly?” *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, p.1-6 IEEE

Almehmadi, T. Alsolami, S. (2019). “Password security in organizations: User attitudes and behaviors regarding password strength” *Advances in Intelligent Systems and Computing*, vol 800, p.9-13

Apple Inc. (16 mars 2022). “Ställa in iCloud-nyckelring” https://support.apple.com/sv-se/HT204085

Bain, Z.L. Hayden, M. Sneesby, S. (2010). “An empirical study of user authentication: The perceptions versus practice of strong passwords” *Issues in information systems*, p.256-265

Brown, A.S. Bracken, E. Zoccoli, S. Douglas, K. (2004). “Generating and remembering passwords” *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition*, vol 18, no 6, p.641-651

DashLane Inc. (2022). “Password Manager App for Home, Mobile, Business”, https://www.dashlane.com

Duggan, G.B. Johnson, H. Grawemeyer, B. (2012). “Rational security: modelling everyday password use” *International journal of human-computer studies*, vol 70, no 6, p.415-431

Gaddis, G.M. Gaddis, M.L. (1990). “Introduction to biostatistics: Part 5, Statistical inference techniques for hypothesis testing with nonparametric data” *Annals of emergency medicine*, vol 19, no 9, p.1054-1059

Gasti, P. Rasmussen, K.B. (2012). “On the Security of Password Manager Database Formats” *Computer Security - ESORICS 2012*, p.770-787, Springer Verlag, Berlin, Heidelberg

IBM. (2022). “IBM SPSS Software”, https://www.ibm.com/analytics/spss-statistics-software

Internetstiftelsen. (2021). “Svenskarna och internet 2021” Internetstiftelsen

Ion, I. Reeder, R. Consolvo, S. (2015). “‘...No one can hack my mind’: Comparing expert and non-expert security practices” *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security*, p.327-346

Ives, B. Walsh, K.R. Schneider, H. (2004). “The domino effect of password reuse” *Communications of the ACM*, vol 47 no 4, p.75-78

Jarecki, S. Krawczyk, H. Shirvanian, M. Saxena, N. (2018). “Two-factor authentication with end-to-end password security” *IACR International Workshop on Public Key Cryptography*, p.431-461 Springer, Cham

Kamat, A. Tomar, C. Tainwala, A. Akram, S. (2018). “Performance analysis and survey on security of password managers and various schemes of p2p models” *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, p.23-26 IEEE

LastPass US. (2022). “The best way to manage passwords”, https://www.lastpass.com/how-lastpass-works

Ma, W. Campbell, J. Tran, D. Kleeman, D. (2010). “Password entropy and password quality” *2010 Fourth International Conference on Network and System Security*, p.583-587

Mayer, P. Volkamer, M. (2018). “Addressing misconceptions about password security effectively” *STAST '17: Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, p.16–27

Nyman, A. (2016). “Skydda dig mot bedragare” Internetstiftelsen https://internetstiftelsen.se/app/uploads/2021/01/skydda-dig-mot-bedragare.pdf

Oates, B.J. (2006). “Researching information systems and computing” Sage Publications, London; Thousand Oaks, Calif

Pensionsmyndigheten. (2022). “Korta pensionsfakta” Pensionsmyndigheten https://www.pensionsmyndigheten.se/nyheter-och-press/pressrum/kortapensionsfakta

Ray, H. Wolf, F. Kuber, R. Aviv, A.J. (2021). “Why older adults (Don't) use password managers” *30th USENIX Security Symposium (USENIX Security 21)*, p.73-90

Reichl, D. (2022). “KeePass Password Safe”, https://keepass.info

Lowry, R. (2022). “VassarStats: Statistical Computation Web Site”, http://vassarstats.net

Samonas, S. Coss, D. (2014). “The CIA strikes back: Redefining confidentiality, integrity and availability in security.” *Journal of Information System Security*, vol 10, no 3, p.21-45

Shay, R. Komanduri, S. Kelley, P.G. Leon, P.G. Mazurek, M.L. Bauer, L. Cranor, L.F. (2010). “Encountering stronger password requirements: user attitudes and behaviors” *Proceedings of the sixth symposium on usable privacy and security*, p.1-20

van der Ham, J. (2021). “Toward a Better Understanding of “Cybersecurity”” *Digital Threats: Research and Practice*, vol 2, no 3, p.1-3

Yates, D. Moore, D. McCabe, G. (1999). ”The Practice of Statistics” (1 uppl.) New York: Freeman

Zhao, R. Yue, C. Sun, K. (2013). “A security analysis of two commercial browser and cloud based password managers” *2013 International Conference on Social Computing* p.448-453 IEEE

8 Bilagor

8.1 Enkätundersökning

Hur medveten är du kring lösenordssäkerhet och lösenordshantering?

Hej!

Jag skriver just nu min c-uppsats i ämnet informationssystem och genomför därför en enkätundersökning kring hur man ser på och hanterar lösenord i olika åldrar.

Du får jättegärna hjälpa mig med uppsatsen genom att fylla i enkäten och du är helt anonym när du gör det. Svaren sparas som längst till uppsatsen är godkänd.

Det är totalt 16 frågor och du kan bara välja ett alternativ per fråga.

Tack på förhand!

Josefin Angerbjörn

1. Hur gammal är du?*

_____

2. Hur ofta använder du en smartphone, dator eller surfplatta?*

- ☐ Varje dag.
- ☐ Någon eller några gånger i veckan.
- ☐ Någon eller några gånger i månaden.
- ☐ Någon eller några gånger per år.
- ☐ Aldrig.

3. Hur många tjänster använder du per vecka som kräver inloggning med hjälp av lösenord?*

- ☐ 0-5
- ☐ 6-10
- ☐ 11-15
- ☐ 16 eller fler

4. Anser du att du själv har en medvetenhet kring vad som gör ett lösenord säkert?*

- ☐ Ja
- ☐ Nej
- ☐ Till viss del.

5. Har du medvetet gett någon i din närhet tillgång till ett/flera av dina lösenord?*

- ☐ Ja
- ☐ Nej

6. Har du lämnat ut ett/flera av dina lösenord till någon som kontaktade dig från en myndighet, bank, företag eller liknande vid något tillfälle?*

- ☐ Ja
- ☐ Nej

7. Är du extra mån om att välja ett säkert lösenord till ditt mejlkonto?*

- ☐ Ja
- ☐ Nej

8. Händer det att du återanvänder samma lösenord på flera ställen?*

- ☐ Ja
- ☐ Nej

9. Har du som vana att ta med någon form av personlig information i dina lösenord, såsom din adress, namnet på ditt husdjur, ett smeknamn eller liknande?*

- ☐ Ja
- ☐ Nej

10. Förvarar du något av eller alla dina lösenord på ett ställe där andra kan komma åt och se dem/ändra dem?*

- ☐ Ja
- ☐ Nej

11. Hur går du tillväga när du skapar nya lösenord?*

- ☐ Jag slumpar fram dem själv eller med hjälp av ett program.
- ☐ Jag hittar själv på dem med hjälp av ord jag lätt kommer ihåg.
- ☐ Annat

12. Använder du ett enligt dig strukturerat sätt för att hålla ordning på dina lösenord?*

- ☐ Ja

☐ Nej

13. Vet du vad en lösenordshanterare är?*

☐ Ja, jag är väl medveten om vad det är.
☐ Ja, men bara till viss del.
☐ Nej

14. Vet du vad tvåfaktorsautentisering är?*

☐ Ja, jag är väl medveten om vad det är.
☐ Ja, men bara till viss del.
☐ Nej

15. Händer det att du använder dig av tvåfaktorsautentisering när det finns tillgängligt?*

☐ Ja
☐ Nej
☐ Jag vet inte vad tvåfaktorsautentisering är.

16. Skulle du vara intresserad av att börja använda en lösenordshanterare*? *En lösenordshanterare är ett program som lagrar alla dina lösenord och som du får åtkomst till genom att bara minnas ett starkt lösenord.*

☐ Ja
☐ Nej
☐ Jag använder mig redan av en lösenordshanterare.

8.2 Statistiska uträkningar

4.

Anser du att du själv har en medvetenhet kring vad som gör ett lösenord säkert?

Ålder		Ja	Till viss del	Nej	Total
65 år och äldre	Count	6	10	2	18
	Share	33,3 %	55,6 %	11,1 %	100 %
Under 65 år	Count	27	20	1	48
	Share	56,3 %	41,7 %	2,1 %	100 %
Total	Count	33	30	3	66
	Share	50,0 %	45,5 %	4,5 %	100 %

Test Results

	Value	Exact Sig. (2-sided)
Fisher's Exact Test		0,113
N of Valid Cases	66	

5.

Har du medvetet gett någon i din närhet tillgång till ett/flera av dina lösenord?

Ålder		Ja	Nej	Total
65 år och äldre	Count	14	4	18
	Share	77,8 %	22,2 %	100 %
Under 65 år	Count	37	11	48
	Share	77,1 %	22,9 %	100 %
Total	Count	51	15	66
	Share	77,3 %	22,7 %	100 %

Test Results

	Value	Exact Sig. (2-sided)
Fisher's Exact Test		1
N of Valid Cases	66	

6.

Har du lämnat ut ett/flera av dina lösenord till någon som kontaktade dig från en myndighet, bank, företag eller liknande vid något tillfälle?

Ålder		Ja	Nej	Total
65 år och äldre	Count	0	18	18
	Share	0,0 %	100,0 %	100 %
Under 65 år	Count	2	46	48
	Share	4,2 %	95,8 %	100 %
Total	Count	2	64	66
	Share	3,0 %	97,0 %	100 %

Test Results

	Value	Exact Sig. (2-sided)
Fisher's Exact Test		1
N of Valid Cases	66	

7.

Är du extra mån om att välja ett säkert lösenord till ditt mejlkonto?

Ålder		Ja	Nej	Total
65 år och äldre	Count	12	6	18
	Share	66,7 %	33,3 %	100 %
Under 65 år	Count	31	17	48
	Share	64,6 %	35,4 %	100 %
Total	Count	43	23	66
	Share	65,2 %	34,8 %	100 %

Test Results

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	0,025[a]	1	0,874
N of Valid Cases	66		

a. 0 cells (0%) have expected count less than 5. The minimum expected count is 6,27.

8.

Händer det att du återanvänder samma lösenord på flera ställen?

Ålder		Ja	Nej	Total
65 år och äldre	Count	15	3	18
	Share	83,3 %	16,7 %	100 %
Under 65 år	Count	42	6	48
	Share	87,5 %	12,5 %	100 %
Total	Count	57	9	66
	Share	86,4 %	13,6 %	100 %

Test Results

	Value	Exact Sig. (2-sided)
Fisher's Exact Test		0,7
N of Valid Cases	66	

9.

Har du som vana att ta med någon form av personlig information i dina lösenord, såsom din adress, namnet på ditt husdjur, ett smeknamn eller liknande?

Ålder		Ja	Nej	Total
65 år och äldre	Count	4	14	18
	Share	22,2 %	77,8 %	100 %
Under 65 år	Count	19	29	48
	Share	39,6 %	60,4 %	100 %
Total	Count	23	43	66
	Share	34,8 %	65,2 %	100 %

Test Results

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1,738[a]	1	0,187
N of Valid Cases	66		

a. 0 cells (0%) have expected count less than 5. The minimum expected count is 6,27.

10.

Förvarar du något av eller alla dina lösenord på ett ställe där andra kan komma åt och se dem/ändra dem?

Ålder		Ja	Nej	Vet inte.	Total
65 år och äldre	Count	1	15	2	18
	Share	5,6 %	83,3 %	11,1 %	100 %
Under 65 år	Count	12	35	1	48
	Share	25,0 %	72,9 %	2,1 %	100 %
Total	Count	13	50	3	66
	Share	19,7 %	75,8 %	4,5 %	100 %

Test Results

	Value	Exact Sig. (2-sided)
Fisher's Exact Test		0,071
N of Valid Cases	66	

11.

Hur går du tillväga när du skapar nya lösenord?

Ålder		Jag hittar själv på dem med hjälp av ord jag lätt kommer ihåg.	Jag slumpar fram dem själv eller med hjälp av ett program.	Annat.	Total
65 år och äldre	Count	16	1	1	18
	Share	88,9 %	5,6 %	5,6 %	100 %
Under 65 år	Count	37	4	7	48
	Share	77,1 %	8,3 %	14,6 %	100 %
Total	Count	53	5	8	66
	Share	80,3 %	7,6 %	12,1 %	100 %

Test Results

	Value	Exact Sig. (2-sided)
Fisher's Exact Test		0,676
N of Valid Cases	66	

12.

Använder du ett enligt dig strukturerat sätt för att hålla ordning på dina lösenord?

Ålder		Ja	Nej	Total
65 år och äldre	Count	13	5	18
	Share	72,2 %	27,8 %	100 %
Under 65 år	Count	31	17	48
	Share	64,6 %	35,4 %	100 %
Total	Count	44	22	66
	Share	66,7 %	33,3 %	100 %

Test Results

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	0,344[a]	1	0,558
N of Valid Cases	66		

a. 0 cells (0%) have expected count less than 5. The minimum expected count is 6,00.

13.

Vet du vad en lösenordshanterare är?

Ålder		Ja, jag är väl medveten om vad det är.	Ja, men bara till viss del.	Nej	Total
65 år och äldre	Count	3	7	8	18
	Share	16,7 %	38,9 %	44,4 %	100 %
Under 65 år	Count	18	16	14	48
	Share	37,5 %	33,3 %	29,2 %	100 %
Total	Count	21	23	22	66
	Share	31,8 %	34,8 %	33,3 %	100 %

Test Results

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2,818[a]	2	0,244
N of Valid Cases	66		

a. 0 cells (0%) have expected count less than 5. The minimum expected count is 5,73.

14.

Vet du vad tvåfaktorsautentisering är?

Ålder		Ja, jag är väl medveten om vad det är	Ja, men bara till viss del.	Nej	Total
65 år och äldre	Count	1	3	14	18
	Share	5,6 %	16,7 %	77,8 %	100 %
Under 65 år	Count	29	13	6	48
	Share	60,4 %	27,1 %	12,5 %	100 %
Total	Count	30	16	20	66
	Share	45,5 %	24,2 %	30,3 %	100 %

Test Results

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	27,662[a]	2	<0,001
N of Valid Cases	66		

a. 1 cells (16,7%) have expected count less than 5. The minimum expected count is 4.36.

15.

Händer det att du använder dig av tvåfaktorsautentisering när det finns tillgängligt?

Ålder		Ja	Nej	Jag vet inte vad tvåfaktorsautentisering är.	Total
65 år och äldre	Count	1	3	14	18
	Share	5,6 %	16,7 %	77,8 %	100 %
Under 65 år	Count	33	10	5	48
	Share	68,8 %	20,8 %	10,4 %	100 %
Total	Count	34	13	19	66
	Share	51,5 %	19,7 %	28,8 %	100 %

Test Results

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	30,897[a]	2	<0,001
N of Valid Cases	66		

a. 1 cells (16,7%) have expected count less than 5. The minimum expected count is 3,55.

16.

Skulle du vara intresserad av att börja använda en lösenordshanterare*? *En lösenordshanterare är ett program som lagrar alla dina lösenord och som du får åtkomst till genom att bara minnas ett starkt lösenord.

Ålder		Ja	Nej	Jag använder mig redan av en lösenordshanterare.	Total
65 år och äldre	Count	5	11	2	18
	Share	27,8 %	61,1 %	11,1 %	100 %
Under 65 år	Count	27	11	10	48
	Share	56,3 %	22,9 %	20,8 %	100 %
Total	Count	32	22	12	66
	Share	48,5 %	33,3 %	18,2 %	100 %

Test Results

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8,599[a]	2	0,014
N of Valid Cases	66		

a. 1 cells (16,7%) have expected count less than 5. The minimum expected count is 3,27.