UNIVERSITY WEST
Institutionen för ekonomi och IT
Avdelningen för informatik

Cybersäkerhet: mellan kunskap och beteende

- En kvalitativ studie om svenska högskolestudenters Cybersäkerhetsmedvetenhet och riskbeteenden

Cybersecurity: Between knowledge and behaviour

- A qualitative study on Swedish university students' cybersecurity awareness and risk behaviours

Författare

Isra Haioty & Zubayer Alam

Kandidatuppsats, 15 Hp

Examensarbete i informatik, EXI500

Vårterminen 2024

Handledare: Lars Svensson

Examinator: Fatemeh Saadatmand

Abstract

Swedish society and the world at large have moved towards a digital direction characterized by innovation and development, which has provided mankind with ease and comfort. Despite these positive aspects of digitalization there has grown criminal and dark elements designated to take advantage of the vulnerabilities that which digitalization brings. This raises questions of IT security and what role this has under the current digitalization of society. Humans within companies make up a weak link regarding cybersecurity and students are an attractive target for IT attackers. It therefore has been relevant to study the cybersecurity awareness among Swedish university students. To conduct this, Swedish students within IT and computer science have been contacted and through a qualitative approach the student's thoughts and perception have been analyzed by semi-structured interviews. The results show that the students have a decent awareness of cybersecurity and know of the most common attacks within an individual level. The result also shows that many of the students previously have been afflicted by an IT attack which has been a reason for increased cybersecurity awareness and safe behavior.

Keywords: Cybersecurity, Cybersecurity awareness, Infosec, IT Security, Risk behavior, IT attack, Information Technology, students

Sammanfattning

Det svenska samhället och världen i stort har rört sig mot en digitaliserad riktning som karaktäriseras av innovation och utveckling, vilket har underlättat och försett bekvämlighet för människan. Trots dessa positiva aspekter av digital utveckling har det i skuggan av dessa vuxit fram kriminella och mörka element för att utnyttja de sårbarheter det digitala medför. Detta ställer frågor kring IT säkerhet och vilken roll detta har under den pågående digitaliseringen av samhället. Människor utgör en svag länk inom företag vad avser IT säkerhet och studenter utgör en attraktiv måltavla för IT angripare. Av denna anledning har det varit relevant att undersöka cybersäkerhetsmedvetenheten bland svenska universitetsstudenter. För att utföra detta har svenska studenter inom IT och datavetenskap kontaktats och genom en kvalitativt ansats har studenternas tankar och uppfattningar kring IT säkerhet och IT attacker analyserats genom semistrukturerade intervjuer. Resultatet visar att studenterna har en allmänt god kännedom om cybersäkerhet och att de känner till de mest förekommande IT attackerna på individnivå. Resultatet visar även att många av studenterna tidigare hade utsatts för IT attacker vilket varit en anledning till en ökad cybersäkerhetsmedvetenhet och säkert beteende.

Nyckelord: Cybersäkerhet, Cybersäkerhetsmedvetenhet, IT-säkerhet, Riskbeteende, IT-attack, Informationsteknologi, studenter

Förord

Vi vill börja med att tacka våra familjer som har stöttat oss under dessa 3 intensiva år av studier utan vars hjälp detta arbete och utbildningsgången inte hade varit möjligt. Vi vill även ta tillfället i akt och tacka vår handledare Lars Svensson för hans engagemang och positiva feedback. Slutligen vill vi tacka alla som deltog i våra intervjuer.

Zubayer och Isra

Begreppslista

Informationssäkerhet – Informationssäkerhet omfattar åtgärder och rutiner som implementeras för att skydda information från olika hot, attacker och intrång. Detta innefattar bland annat säkerhet från obehörig åtkomst, användning, modifiering eller förstörelse av data.

Cybersäkerhet – Cybersäkerhet fokuserar specifikt på att skydda digitala system, nätverk och data från cyberhot och att implementera säkerhetsåtgärder för att motarbeta attacker. Cyberattacker kan till exempel vara malware-infektioner, phishing-attacker, DOS-attacker, bruteforce och man-in-the-middle attacker.

Cybersäkerhetsmedvetenhet – Cybersäkerhetsmedvetenhet är förståelsen om informationssäkerhet och hur man förhåller sig till det för att skydda sig mot just cyber-attacker. Den omfattar flera delar som att surfa säkerhet, integritetsskydd och säkerhetsåtgärder mot cyberhot.

IT-attack – Olika cyberangrepp i syfte att störa, skada eller få obehörig tillgång till system.

Social Engineering – Social Engineering är en typ av cyberattack som bygger på psykologiska faktorer och användaren som verktyg. Hackaren använder sig av manipulation för att få användarna att utföra en handling eller dela med sig av känslig information. En typ av Social engineering attack är Phishing, så kallat nätfiske.

Phishing (nätfiske) – Phishing är en teknik som syftar på att få offret att klicka på skadliga länkar eller ladda ner en bilaga för att försöka begära personlig information för att sedan kunna stjäla känsliga data, identitet eller pengar.

Darknet – En del av internet som kräver en speciell typ av mjukvara för att få tillgång till. Oftast associerat med en svart marknad där kriminella handlingar begås.

SSL - Secure sockets layer. Kryptering vilket möjliggör att säkra kommunikationen över internet.

Innehållsförteckning

1 Introduktion

De senaste åren har antalet cyberattacker ökat markant. Mellan år 2022 och 2023 sågs den största ökningen av dessa hot i Europa. Europeiska unionens byrå för cybersäkerhet, ENISA, har rapporterat en lista på de 8 största hoten. Bland dessa 8 cyberhot och attacker rankas malware och Social Engineering högst (ENISA, 2023a). I en annan rapport av ENISA (2023b) förklarar de att år 2030 förväntas en stor ökning av smarta enheter som samlar beteendedata och användarprofiler. Angripare kan använda denna data för att utföra attacker genom manipulativa metoder, det vi kallar för Social Engineering. Med denna ökning av smarta enheter behövs det fler medel för att säkra känsliga data från angripare eftersom dessa kan komma att ha en påverkan på individ- och nationellnivå (ENISA, 2023b).

September 2023 föreslog den svenska regeringen att Cybercampus Sverige skall inrättas med syftet att stärka forskning och kompetensförsörjning inom cybersäkerhet i landet (Regeringskansliet, 2023). Detta är ett nationellt initiativ, med samarbete mellan Försvarsmakten, Kungliga Tekniska högskolan (KTH), Myndigheten för samhällsskydd och beredskap (MSB) samt industrin. På grund av rådande situation med ökad digitalisering och ökade it-attacker har ett behov identifierats för att säkra vårt digitala landskap. Målet med Cybercampus är att möjliggöra forskning, innovation och utbildning för cybersäkerhet, för att stärka Sveriges cybersäkerhet och motståndskraft (KTH, 2024).

Genom en kvalitativ ansats ämnar denna studie att djupgående undersöka och utvärdera cybersäkerhetsmedvetenheten bland svenska IT och datavetenskapsstudenter inom högskolenivå. Genom att fokusera på de främsta attackerna som ENISA identifierat ämnar studien utforska hur detta påverkar svenska studenter. Den kvalitativa metoden möjliggör en djup förståelse av studenternas uppfattning och beteenden, vilket är av stor vikt för att identifiera sårbarheter och relaterade förebyggande strategier. Genom detta bidrag hoppas vi att bidra till forskningen inom cybersäkerhet.

1.1 Bakgrund

Cyberhot är på framfarten och utvecklas till att bestå av organiserade kriminella grupper vilket utgör seriösa hot mot global säkerhet. Denna utveckling är en följd av att samtiden karaktäriseras av modern teknik och dess alltmer ökande antal av användare, vilket drastiskt påverkat människors sätt att leva, i synnerhet kommunicering och informationshantering (Alharbi & Tassadiq, 2021). I den antika världen uppfattades den trojanska hästen vara en militärisk fälla som skickades till fienden utsmyckat till en present men som faktiskt var en fälla. När den massiva trähästen hade tagit sig förbi fiendens portar exploderade den inifrån, till trojanernas förvåning, och en stor mängd av de bästa grekiska soldater som hade gömt sig inuti den stora hästen befanns sig nu i den allra svagaste och känsligaste punkten av fienden, och kunde öppna Trojas portar för att erövra staden (Pfleeger m.fl., 2015). I den antika världen må begreppet ”trojansk häst” blivit uppfattat på detta sätt. Den moderna uppfattningen av detta begrepp skiljer sig däremot drastiskt. Pfleeger m.fl. (2015) menar att den moderna beteckningen av trojansk häst är en beskrivning på en form av IT-attack som ytligt ser ofarlig och säker ut men likt trähästen innehåller och döljer en skadlig effekt.

IT-attacker kan initieras av olika anledningar. Människor har ofta olika motiv bakom deras attacker. Ett av dessa är det ekonomiska motivet. Pfleeger m.fl. (2015) skriver bland annat att en global internetrapport som fokuserade på internethot kom till underfund med att de mest förekommande föremålen erbjudna till försäljning åren 2008 och 2009 på ”undergroundhemsidor” (s.51) var kreditkortsnummer följt av bankkontosiffror och e-postkonton. Andra motiv inkluderar politiska, en strävan efter prestige och status eller till och med terrorrelaterade.

Övrig forskning visar även att det årligen sker en stor mängd IT-attacker med betydande finansiell påverkan (Albayrak & Bagci, 2022). Flera faktorer bidrar till den alltmer ökande framfarten av IT-attacker, men det kommer ner värdet gärningsmännen får ut av det. De finansiella motiven bakom cyberattacker materialiseras genom olika sätt, bland annat stjäls personliga data och säljs vidare på darknet (Alharbi & Tassadiq, 2021). Dessa finansiella aspekter gör cybersäkerhet till ett högaktuellt ämne.

Ytterligare forskning (Dieye m.fl., 2020) visar att finanssektorn är bland det attraktivaste för cyberkriminella att välja som måltavla, vilket påverkat många länder inom en makroekonomisk nivå. Dieye m.fl. (2020) redogör för den ekonomiska förlusten inom finanssektorn för olika västerländska länder och presenterar förlusten för ett antal givna länder. Priset för IT-attacker för USA har uppgått ända upp till 14 miljoner dollar inom finanssektorn själv.

2007 drabbades den svenska banken Nordea av en cyberattack (BBC, 2007). Detta ledde till att banken förlorade ca 8miljoner SEK och 250 kunder påverkades. Cyberattacken utlöstes genom ett virus som skickades via e-post. Kunderna trodde alltså att mejlet kom från en betrodd avsändare, men så var inte fallet. Genom att öppna mejlet och installera programmet laddades det ner ett virus som gav angriparen tillgång till användarnas bankuppgifter. Detta är ett av flera exempel av hur enkelt cyberattacker kan drabba individer och organisationer samt demonstrerar hur sårbara vi är.

Cybersäkerhetsmedvetenhet anses vara viktigt att förstå av flera olika anledningar. Begreppet definieras som en kombination av kunskap, attityd och aktivt agerande för att skyddas från cyberhot (Shukla m.fl.,2022). Det ger kunskap till slutanvändare om både säkerhetsproblem, cyberattacker, hot och åtgärder. De flesta attacker idag beror på av mänskliga faktorer till följd av bristande säkerhetsmedvetenhet. Trots att teknologiska metoder och säkerhetsåtgärder må ha vidtagits så kan slutanvändaren vara faktorn till intrång och sårbarhet. Genom att öka användarnas förståelse om cyberrisker och vilka skyddsåtgärder som kan vidtas, kan cyberattacker förebyggas (Arachchilage & Love, 2014).

Tidigare forskning har påvisat att det finns brist om cybersäkerhetsmedvetenhet bland högskolestudenter i flera olika regioner runt om i världen. Studier som har utförts i Saudiarabien och Peru visar att det finns en allmän brist om säkerhetsmedvetenhet bland högskolestudenter och fastän studenterna hade en viss eller hög förståelse för cyberrisker så saknade de en mer djupgående kunskap om säkerhetsåtgärder för att effektivt bemöta cyberhot och attacker. Flera faktorer identifierades som utlösaren till cyberattacker där den

gemensamma nämnaren var den mänskliga faktorn genom bland annat användning av offentlig Wi-Fi, svag lösenordshantering och interaktion med okända länkar (Alharbi & Tassaddiq, 2021; Revilla m.fl., 2023).

1.2 Problembeskrivning

Efter studiens litteraturgranskning kring liknande forskning inom Europa, hittades det endast en jämförelsestudie som genomfördes i Portugal och Polen (Oliveira m.fl., 2023). Detta kan indikera att det finns ett kunskapsgap inom forskning om cybersäkerhetsmedvetenhet bland nordiska och svenska högskolestudenter. Det är viktigt att förstå cybersäkerhetsmedvetenheten bland denna målgrupp för att säkerställa en trygg och säker användning av digitala verktyg samt för att främja en kultur med hög cybersäkerhetsmedvetenhet. Dessutom anses denna målgrupp vara en högrisk samt måltavla för angripare, bland annat på grund av deras höga datoranvändning både för privatbruk och inom sin institution (Alharbi & Tassaddiq, 2021).

Det blir viktigt att analysera högskolestudenters cybersäkerhetsmedvetenhet eftersom de med störst sannolikhet kommer att bli framtida anställda i olika verksamheter. I allt högre utsträckning använder verksamheter digitala system och förlitas sig på det, därmed måste yrkesverksamma ha en stark förståelse för cybersäkerhet för att skydda data, känslig information och minska risker för cyberattacker (An m.fl., 2022). Genom att förbättra kunskapen om cybersäkerhet kan vi skapa en säkrare digital miljö för all form av data som vi hanterar dagligen, både i privatbruk, inom tjänsten och i andra sammanhang.

1.3 Syfte & frågeställning

Då inga omfattande nordiska och svenska forskningar hittats inom forskningsområdet, tyder detta på att det finns ett kunskapsgap. Därmed ämnar denna studie genom en kvalitativ metod att undersöka och utvärdera svenska högskolestudenters cybersäkerhetsmedvetenhet, attityder och beteenden genom att besvara följande frågeställning:

Hur medvetna är svenska högskolestudenter om informationssäkerhet och cyberattacker och hur relaterar detta till deras faktiska beteenden?

1.4 Avgränsning

Målgruppen har avgränsats till att endast bestå utav svenska högskolestudenter som studerar en kandidatexamen inom IT och datavetenskap. Vi har därmed respondenter som studerar till mjukvaruingenjör, dataingenjör, systemutvecklare samt nätverkssäkerhet. Urvalet av dessa respondenter är från olika lärosäten inklusive Blekinge Tekniska Högskolan, Högskolan Väst och Kungliga Tekniska Högskolan. Vi har valt att fokusera på de mest förekommande typerna av cyberattacker för individer år 2023 samt rekommenderade skyddsåtgärder kopplade till det. Denna avgränsning valdes eftersom de är mest relevant för målgruppen samt på grund av studiens tidsomfång.

2 Teoretisk referensram

2.1 Tidigare forskning

2.1.1 Säkerhetsmedvetenhet i andra länder

I Silicon Valley, USA utfördes en studie som undersökte cybersäkerhetsmedvetenhet och attityder bland högskolestudenter från två universitet. Studien visade att studenterna inte följde säkerhetsåtgärder. De hade sällan starka lösenord, delade privat information och använde universitetets offentliga nätverk utan försiktighet. Studenterna visste att deras beteenden inte var helt säkra men trots detta var de bekväma med att dela känsliga data via universitetets offentliga nätverk, på grund av att de inte visste hur de kunde skydda sig på bästa möjliga sätt, (Moallem, 2019). Denna studie visar att kunskap om cybersäkerhet inte garanterar säkert beteende. Enligt Slusky och Partow- Navid (2012) är bristen på kunskap inte huvudproblemet utan det är snarare studenternas beteende och attityder, vilket Shukla m.fl. (2022) kallar för ”aktivt agerande”. Detta är faktorer som visar sig i flera av de andra studierna som har granskats.

I Alharbi & Tassadiqs (2021) studie som utfördes i Majmaah University i Riyadh, Saudiarabien visade att trots att 92% av respondenterna hade deltagit på en formell utbildning om IT-säkerhet, visade att studenterna hade en begränsad kunskap om cybersäkerhet och hur man skyddar sina enheter. Majoriteten använde bland annat inte antivirusprogram, hade svag lösenordshantering på grund av lathet och visste inte varför säkerhetsåtgärder skulle vara viktiga. Alharbi och Tassadiq (2021) menar att formell utbildning om cybersäkerhet inte är tillräckligt för att bidra med cybersäkerhetsmedvetenhet åt studenterna, utan att det krävs en kombination av metoder som bland annat spel-baserat lärande, träning, intervjuer och utbildning från ung ålder.

I en europeisk studie som utfördes bland polska och portugisiska universitetsstudenter visar resultatet att polska studenter visade en högre kunskap om cybersäkerhet men att de inte implementerade säkerhetsåtgärder ofta (Oliveira m.fl., 2023). Portugisiska studenter visade dock på en högre grad av implementering av skyddsåtgärder, men att deras kunskap om cyberattacker var lägre. Oliveira m.fl., (2023) förklarar att en orsak till detta det kan bero på att universiteten har olika lärmetoder i dessa länder.

2.2 Definition av informationssäkerhet och cybersäkerhet

Termerna informationssäkerhet och cybersäkerhet är två begrepp som har använts nästintill som synonymer av flera författare. Informationssäkerhet omfattar åtgärder och rutiner som implementeras för att skydda information från olika hot, attacker och intrång. Detta innefattar bland annat säkerhet från obehörig åtkomst, användning, modifiering eller förstörelse av data. Grunden av informationssäkerhet är CIA-begreppet som står för Confidentiality, Integrity och Availability. På svenska står detta för sekretess, tillförlitlighet och tillgänglighet av data (Liu m.fl. 2020). Detta betyder att all data som hanteras skall vara sekretessbelagd och förhindra

obehöriga från att få tillgång till det. Tillförlitlighet innebär att data inte ska modifieras av obehöriga och tillgänglighet handlar om att data skall vara tillgänglig och nåbar vid behov.

Cybersäkerhet fokuserar specifikt på att skydda digitala system, nätverk och data från cyberhot och att implementera säkerhetsåtgärder för att motarbeta attacker (ISO 20252). Cyberattacker kan till exempel vara malware-infektioner, phishing-attacker, social engineering, DOS-attacker, bruteforce och man-in-the-middle attacker.

FN:s specialiserade organ för information och kommunikationsteknologi, International Telecommunications Union (ITU) definierar cybersäkerhet som följande:

” Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets” (ITU, 2024)

ISO 20252:2019(en) definition av cybersäkerhet:

“protection of an IT-system from the attack (3.2) or damage to its hardware, software or information, as well as from disruption or misdirection of the services it provides.”

ISO /TR 22100-4:2018(en) definition av informationssäkerhet:

“preservation of confidentiality, integrity and availability of information”

2.3 Definition av cybersäkerhetsmedvetenhet

Rahim m.fl. (2015) förklarar att cybersäkerhetsmedvetenhet är förståelsen om informationssäkerhet och hur man förhåller sig till det för att skydda sig mot just cyberattacker. Den omfattar flera delar som att surfa säkerhet, integritetsskydd och säkerhetsåtgärder mot cyberhot. Denna säkerhetsmedvetenhet är viktig för alla som hanterar data på olika sätt. Bland annat är den av stor vikt bland universitetsstudenter, mjukvaruutvecklare och för anställda och organisationer (Alharbi & Tassaddiq, 2021, An m.fl., 2022). Cybersäkerhetsmedvetenhet understryks av dess inverkan på att minska cyberhot, förbättra säkerhetsrutiner och bidrar till att främja en kultur av säkerhetsmedvetenhet bland både individer och organisationer.

Corallo m.fl. (2022) definierar termen inom ramen för kunskap. Kunskap att förstå cyberhot och cyberattacker samt vara medveten om dess risker. Däremot definierar Shukla m.fl. (2022) cybersäkerhetsmedvetenhet som en kombination av kunskap, attityd och aktivt agerande för att skyddas från cyberhot. Shukla m.fl. (2022) utgår från den allmänna definitionen av medvetenhet och har därtill lagt till aktivt agerande. Med aktivt agerande menas att användarna inte bara har kunskapen om cybersäkerhet, utan även försöker implementera säkerhetsåtgärder, rutiner och minska riskerna för cyberattacker. Detta kan till exempel vara att de har virusprogram nedladdat, uppdaterade mjukvaror, surfar säkert eller inte öppnar länkar från opålitliga avsändare. I denna studie väljer vi att använda den senare definitionen av Shukla m.fl. (2022).

2.3.1 Varför är cybersäkerhetsmedvetenhet viktigt?

I takt med att cyberattacker har ökat den senaste tiden har studenter och universitet blivit en attraktiv måltavla för hackare. Universitet och högskolor utsätts för allt fler attacker där studenter utgör bland de mest sårbara tillgångarna för akademiska institutioner, som har känsliga data att skydda. Detta är även relevant utifrån ett företagsperspektiv eftersom personalen inom företag oftast utgör den svagaste länken (Alharbi & Tassaddiq, 2021).

Litteraturgranskningen som utfördes kom med underfund med en brist inom cybersäkerhetsmedvetenhet och implementerandet av detta i flera olika regioner. Tidigare forskningarna visar på brist inom cybersäkerhetsmedvetenhet i bland annat Silicon valley (USA), Bangladesh, Turkiet, Saudiarabien, Peru, Polen och Portugal (Alharbi & Tassaddiq, 2021; Oliveira m.fl., 2023; Revilla m.fl., 2023; Erendor & Yildirim, 2022; Moallem, 2019).

Cybersäkerhetsmedvetenhet blir därför viktigt att förstå. Den ger kunskap till slutanvändare om både säkerhetsproblem, cyberattacker, hot och åtgärder. De flesta attacker idag beror på av mänskliga faktorer till följd av bristande säkerhetsmedvetenhet. Trots att teknologiska metoder och säkerhetsåtgärder har vidtagits så kan slutanvändaren vara den utlösande faktorn till intrång och sårbarhet. Genom att öka användarnas förståelse om cyberrisker och vilka åtgärder som kan tas, kan man förebygga cyberattacker (Arachchilage & Love, 2013; Verizon, 2023; Junger m.fl.,2017).

Shukla m.fl.(2022) förklarar att utbildning från ung ålder inom cybersäkerhetsmedvetenhet kan skapa en kultur inom samhället som motarbetar cyberattacker och hot. Genom att öka cybersäkerhetsmedvetenheten och utbildning inom cybersäkerhet kan vi främja ett säkrare digitalt ekosystem. Detta kommer även att förbereda studenter som skall ut i arbetsmarknaden med rätt färdigheter och kunskap att känna igen hot och ta lämpliga säkerhetsåtgärder. Genom att främja en sådan kultur gynnar det individerna i sina privata liv men skyddar även organisationer.

2.4 Typer av attacker

I detta avsnitt beskrivs olika typer av attacker och skyddsåtgärder som denna studie ämnar fokusera på. De valda attackerna är med i ENISAS lista av de mest förekommande attackerna. (ENISA, 2023a).

2.4.1 Malware

Malware är en skadlig programvara eller kod som har som syfte i att skada eller göra intrång i dator, nätverk eller andra digitala enheter, utan användarens medgivande. Malware är en övergripande term för virus, trojaner, spionprogram, reklamprogram, ransomware och andra skadliga program. Dessa brukar vara gömda i programvaror och får tillgång till en enhet vid nedladdning av ett program eller bilaga. Malware har olika syften och fungerar på lite olika sätt, däremot använder angripare dessa som medel för att antingen radera, modifiera, kryptera data eller övervaka en användares aktivitet (Erbschloe, 2019).

Pfleeger m.fl. (2015) definierar en mängd av begrepp tillhörande Malware och menar att virus innebär skadlig kod som kan replikera sig själv för att sedan passera detta vidare till andra fungerade program. Begreppet myntades eftersom det påminner om ett biologiskt virus genom att bifoga sig till andra fungerade program för att antingen förstöra programmet eller befinna sig inom det. En mask (Worm) å andra sidan skiljer sig genom att vara ett program som sprider sig genom ett nätverk. En mask sprider kopior av sig själv självständigt medan virus sprids genom att bifoga sig till olika program.

Malware har en verklig påverkan på människor och världen i stort, dess påföljder leder till påtagbara konsekvenser. Pfleeger m.fl. (2015) ger verkliga exempel på när skadlig kod har haft en samhällspåverkan. Melissa viruset skickade e-post till kontakterna av en användare vilket ledde till mottagarna trodde att e-posten var autentiskt men som faktiskt spred vidare infektionen till deras kontakter. IloveYou masken skrivs ha påverkat drygt 10 000 servrar vilket resulterade i att 1 av varje 28 e-postmeddelande var en infektion från datormasken. Mask attacken Code Red skrivs att ha haft liknande påverkvan och påverkat användare på drygt 3 miljoner värdar.

Incidenter med infektioner som dessa har ett högt pris vilket kostar mycket pengar och har en tydlig påverkan på användaren såväl som samhället i stort.

2.4.2 Social engineering

Social engineering anses vara den enklaste cyberattacken som de flesta användare råkar ut för. Den bygger på psykologiska faktorer och användaren som verktyg (Erbschloe, 2019). Enligt Verizon’s 2023 Data Breach Investigations rapport beror 72% av dataintrång på grund av mänsklig faktor antingen genom misstag, missbruk av behörighet, användning av stulna inloggningsuppgifter eller genom social engineering (Verizon, 2023).

Angripare använder sig av manipulation för att få användarna att utföra en handling eller dela med sig av känslig information. Social engineering attacker är inte nytt och har funnits väldigt länge. Utifrån ett historiskt perspektiv har kriminella använt sig av manipulation via olika medel som exempelvis reklam, telefonsamtal, brev eller förfalskat sin identitet för att utvinna något. I dagens digitala värld har dessa metoder utvecklats och idag använder sig angripare av bland annat e-post, sms, sociala medier och andra plattformar som spelsidor och reklam (Erbschloe, 2019).

Angripare som använder sig av social engineering metoder utgår ifrån människans sårbarhet. Deras metoder kan bestå av enklare metoder som ”skadliga” länkar där det räcker med ett klick för att aktivera ett virus eller mer avancerade metoder som bygger på att angriparen utger sig för att vara någon eller något offer litar på. Exempel på detta kan vara välkända och betrodda företagsnamn, myndigheter eller en person som användaren känner. Angripare utnyttjar två sårbarheter hos människan: svårigheten att identifiera och att verifiera en källa (Erbschloe, 2019).

2.4.3 Phishing

En av de vanligaste attacker inom Social engineering är Phishing (nätfiske). Det är en metod som bygger på att få offret att klicka på skadliga länkar eller ladda ner en bilaga för att försöka begära personlig information för att sedan kunna stjäla känsliga data, identitet eller pengar. Länken ser ut att komma från en betrodd källa oftast via e-postmeddelande, sms eller andra kanaler. Denna metod brukar användas i kombination med att skapa en känsla av en nödsituation som ökar chansen för mottagaren att agera snabbt (Erbschloe, 2019). Ett exempel på en sådan incident var år 2007 då den svenska banken Nordea utsattes för ett phishing-attack, där angripare förfalskade ett meddelande som skickades ut till Nordeas kunder och fick det att ladda ner ett program. Det programmet innehöll ett virus, så kallat malware. När kunderna hade loggat in på sin bank kunde hackaren stjäla deras information. Cirka 8 miljoner SEK blev stulet och 250 Nordea kunder påverkades genom denna phishing attack (BBC, 2007). Med dessa konsekvenser i åtanke beskrivs skyddsmekanismerna nedan.

2.5 Skyddsmekanismer

Pfleeger m.fl. (2015) ägnar ett helt kapitel åt att diskutera deras rekommendation av tre kraftfulla skyddsmekanismer: identifiering & autentisering, åtkomstkontroll och kryptering. Relevant för studien är identifiering & autentisering.

Pfleeger m.fl. (2015) menar att grunden till datorsäkerhet är kontrollerad tillgång (access), dvs att någon är berättigad åt att utföra en handling på något. För att detta däremot ska funka krävs det att denna ”någon” är en definierad person. Av denna anledning nämns termerna autentisering & identifiering vilket avser processen av att bekräfta en identitet. Skillnaden mellan begreppen ligger i att identifiering är handlingen av att påstå vem en person är och autentisering innebär handlingen av att bevisa den påstådda identifieringen.

- Autentisering för att bekräfta en identitet fungerar genom vetskap av följande tre punkter av en användare: någonting användaren känner till såsom ett PIN kod, någonting fysiskt hos användaren såsom som fingeravtryck eller ansiktsdrag för bildigenkänning. Slutligen nämner Pfleeger m.fl. (2015) något som användaren besitter såsom ID kort eller fysiska nycklar.

2.5.1 Lösenordshantering

I ljuset av kontrollerad tillgång kommer lösenord att diskuteras. Pfleeger m.fl. (2015) skriver att lösenord är den första formen av datorautentisering (computer authentication). Om det goda lösenordet skrivs att den bör utökas av tecken utöver a-z. När lösenord väljs enbart från a-z är det endast 26 möjliga alternativ per bokstav. Genom att addera siffror ökar totala antal alternativ till 36. Om det dessutom används versaler och gemener i kombination med siffror, uppnås upp till 62 olika tecken som kan användas. Den positiva effekten av detta är betydande vid försök att knäcka lösenord genom att testa varje möjlig kombination av tecken. Pfleeger m.fl. (2015) skriver att det skulle ta 100 timmar att testa alla möjliga 6-bokstavsord som endast består av bokstäver i samma storlek, men att testa alla av 6-tecken lösenord innehållande versaler & gemener samt siffror kan ta upp till två år.

Pfleeger m.fl (2015) nämner ytterligare säkerhets principer för att skapa säkra lösenord. Dessa inkluderar:

Att hålla lösenorden långa. Genom att skapa ett långt lösenord minskas sannolikheten att lösenordet kan upptäckas. Det rekommenderas även *att undvika faktiska namn eller ord*, vilket skulle göra det svårare för en angripare att upptäcka lösenordet om det inte återfinns i en ordbok. I stället rekommenderas *att använda en textsträng användaren kan komma ihåg*, genom att stringen har en speciell innebörd till användaren utan att någon annan kan gissa denna speciella innebörd. Stringen ska inte heller vara för uppenbar. För att hantera problemet av att komma ihåg flera olika lösenord åt flera olika tjänster rekommenderas *att använda sig av varianter för lösenord.* Lösenordet kan ha en viss grundstruktur, men sedan baserat på vilken tjänst ett lösenord ska användas till kan lösenordet lägga till något extra som associeras åt den unika tjänsten.

Med dessa principer av lösenordsskapande klargjorda skriver Pfleeger m.fl (2015) om att behålla ett lösenord säkert. Det rekommenderas att ändra lösenordet regelbundet, även om ingenting tyder på att lösenordet blivit kapad. Det finns en ständig fara att en angripare kan ha brutit sig in på ett lösenordssystem och fått tillgång till en gammal lista av lösenord eller aktivt jobbar på att bryta sig in i krypterade listor. Slutligen rekommenderas det att inte dela med sig lösenordet till någon annan. Detta beror på att den enklaste attacken är social engineering. Genom att dela med sig av sitt lösenord till någon annan som påstår sig behöva lösenordet av olika anledningar är risken för att det är en social engineering attack stor.

Ovanstående punkter är vägledande säkerhets principer för att uppnå god lösenordshantering. Pfleeger m.fl. (2015) nämner däremot ett problem. Med hänvisning till psykologisk litteratur menar Pfleeger m.fl. (2015) att det blir jobbigt för användaren att minnas flera lösenord samtidigt för flera olika tjänster. Det är av denna anledning lösenordshanterare (password manager) finns. Pfleeger m.fl. (2015) definierar lösenordshanterare till att vara ett ställe där kunder kan lagra information som de använder i andra hemsidor. Säkerhetssyftet lösenordshanterare uppfyller är att de dels hjälper användaren att skapa starka och säkra lösenord samtidigt som detta lösenord sparas inom denna tjänst – användaren slipper alltså behöva memorera långa & säkra lösenord utan behöver endast logga in på lösenordshanteraren för att få tillgång till sina lösenord. Ett annat alternativ är tvåfaktorsautentisering vilket Pfleeger m.fl. (2015) menar innebär kombinerandet av autentisering mellan användaren och olika mjukvaror.

2.5.2 Antivirus

Enbart god lösenordshantering är inte speciellt effektiv mot malware. Pfleeger m.fl. (2015) skriver att antivirus leverantören McAfee rapporterade om att de kunde identifiera 200 nya typer av malware per minut. Vid början av 2012 hade deras malware bibliotek runt 100 miljoner typer av malware och vid slutet av 2013 hade siffran höjts till 196 miljoner. antivirusprogram och används för att hjälpa mot detta problem genom att identifiera malware. Däremot nämner Pfleeger m.fl. (2015) att det finns brister inom antivirusprogram och att de inte utgör ett totalt skydd mot malware, bland annat nämns en källa som påstod att antivirus program endast fångar upp 45% av all skadlig kod. Detta beror främst på två orsaker. Pfleeger

m.fl. (2015) skriver att den första anledningen beror på naturen av retroperspektiv av antivirusprogram. Antivirusprogram söker efter mönster av igenkända infektioner. Detta innebär att för nya skadliga infektioner som skapas behöver antivirusprogrammen uppdateras i takt med detta. Den andra anledningen beror på att antivirusprogram kämpar med att skilja mellan skadlig och godartad kod på grund av kontinuerliga förändringar och variationer i skadliga kodmönster, vilket gör upptäckter utmanande. Pfleeger m.fl. (2015) menar att antivirusprogram står inför utmaningen att effektivt identifiera skadlig kod, eftersom skaparna av denna kod kontinuerligt justerar och varierar dess struktur för att undgå upptäckt. Detta tvingar fram en ständig anpassning hos antivirusprogrammen, som måste utveckla förmågan att känna igen ett allt större spektrum av komplexa mönster.

2.5.3 Användarvigilans

Pfleeger m.fl. (2015) delar upp åtgärder utifrån ett användarperspektiv och utvecklarperspektiv. Denna del av studien kommer att fokusera på användarperspektivet i enlighet med studiens inriktning. Pfleeger m.fl. (2015) skriver att användaren är den som skadas allra mest av malware infektion, vilket gör det ytterst relevant att användaren först och främst implementerar säkerhetsskydd. Den enklaste åtgärden mot skadlig kod är vad Pfleeger m.fl. (2015) kallar ”hygien” – att användaren inte sysslar med beteenden som möjliggör skadlig kod från första början. Begreppet skrivs att bestå av två komponenter: att blockera vägar för sårbarhet och att undvika kontaminationspunkter.

Pfleeger m.fl. (2015) skriver om försiktighetsåtgärder användaren kan vidta kring mjukvara. Det rekommenderas utifrån ett användarperspektiv att endast använda kommersiell mjukvara från pålitliga och igenkända leverantörer. Detta beror på att sådana företag ofta vill bevara sina rykten vilket skulle kunna rasa bara av en dålig incident. Av denna anledning ser de till att hålla deras produkter virus-fri. Om mjukvara däremot av någon anledning måste laddas ner från källor där det råder frågetecken kring rekommenderas det att först testa mjukvaran på en isolerad dator som inte innehåller känsliga data och som inter kopplad till ett nätverk. För att avgöra om det kan användas på en mindre isolerad dator ska mjukvaran köras på den isolerade datorn med ett antivirusprogram på. Om inga misstänksamheter upptäcks kan det då gå vidare med att installeras på en mindre isolerad dator.

Utifrån ett systemperspektiv rekommenderas att skapa återställbar systembild samt att skapa säkerhetskopior av körbara systemfiler. Genom att göra detta kan rena filer återhämtas och ersättas med korrupta filer om användaren blivit utsatt för virusinfektioner.

I den digitala världen bör användaren bejaka vaksamhet genom insynen att vilken sida som helst kan potentiellt utgöra en skaderisk. Pfleeger m.fl. (2015) skriver att en vaksam surfare bör vara på vakt åt hemsidor som bland annat tillhandhåller smuggelgods, biljettåterförsäljning samt pornografi. Vidare finns det hemsidor vars domän är associerade till länder som Kina, Korea, Indien och Ryssland vilket kräver försiktighet då hemsidor från dessa länder väldigt ofta toppar listan för mest webbsidor med skadlig kod. Bilagor ska även bara öppnas då det är känt att de är säkra. Detta kan vara svårt att avgöra men olika tecken för detta är söka efter källan av bilagan. Om källan är en igenkänd källa med ett udda medelande eller beskrvning, är detta däremot en varningssignal.

2.5.4 VPN

Abbas m.fl. (2023) skriver att VPN (Virtual private networks) spelar en avgörande roll inom affärsprocesser när det gäller att förse med säkerhet och skydd. Detta beror på VPN: er använder sig av tunnlande nätverk över internet som genom kryptografi möjliggör säkerhet och skydd. Skyddsmekanismerna VPN förser med är konfidentialitet, integritet och autenticitet. Detta sker genom att datapaket krypteras innan de transmitteras genom tunneln. Integritet uppnås under processen genom hashningsalgoritmer som upptäcker manipulering under överföringen. Autenticitet mekanismer finns genom av att identifiera användare. Genom ett sådant tillvägagångssätt av säkrade tunnlar genom VPN kan datapaket skyddas från attacker och avlyssning från exempelvis angripare eller regeringen, vilken inte alltid är fallet när en användare vill använda sig av internet genom okrypterad internettrafik (Abbas m. fl, 2023).

Abbas m.fl, (2023) skriver att det finns ett antal nyckelfunktioner VPN: er måste tillhandhålla för att försäkra dess användare med säkerhet och integritet. Bland dessa är:

- Genom ett brett urval av olika IP adresser döljer VPN dess användares data genom krypterade tunnlar vilket bär en annan IP adress.
- Anslutningstillståndet av VPN bryts om användaren inte längre är ansluten till VPN i syfte att okrypterad dataöverföring inte skickas över nätverket.
- Om flera användare är ansluten till en VPN server kan de tolka varandras DNS förfrågningar, alltså namn tilldelade IP adresser. Detta kräver att DNS förfrågningar krypteras likt HTTPS förfrågningar krypteras med SSL.
- Vissa VPN: er lagrar användarens sökaktivitet under lägre tidsperioder, men VPN: er bör påtvinga ”no-logging” policier.
- Inom ett organisationsperspektiv ska det inte krävas VPN installeras på individuella system för varje enskild individ utan VPN ska bli tillgängligt genom att den finns installerat på organisationens router, vilket skulle göra att en anslutning till organisationens nätverk automatiskt ger en fördelarna av VPN säkerhet.
- Det bör finnas ”split tunneling protocol” vilket är en funktion som låter användaren välja vilka föremål som ska skyddas. Detta gör att de icke valda föremålen kan nås utanför de krypterade tunnlarna i snabbare fart.
- Enligt Abbas m.fl, (2023) finns det ett problem med att IP adresser börjar ta slut. För att adressera detta problem finns en ny struktur kallat IPV6 (IP security protocoll version 6) designat för att öka adressrymden och skydda data (Abbas m.fl., 2023; Pfleeger m.fl., 2015). Abbas m.fl, (2023) skriver att ett väldigt viktig funktion av VPN blir därmed att skydda IPv6 från läckage.

2.5.5 Sammanfattning av åtgärder

För att motverka och skydda sig mot cyberattacker är det viktigt att kombinera tekniska lösningar med kunskap. Eftersom angripare använder sig av manipulation mot sina offer, är det högst viktigt att sprida information om dessa metoder och göra användare medvetna om dessa. Man bör utbilda hur dessa attacker fungerar och vad man ska vara uppmärksam mot (Erbschloe, 2019; Shukla m.fl, 2022). Det kan till exempel handla om att vara källkritisk och dubbelkolla avsändarens identitet, aldrig lämna ut sitt lösenord, personlig information eller finansiell information om de kommer från e-postmeddelanden eller sociala medier. Man skall heller inte ladda ner programvaror utan att först säkerställa att sidan är säker.

Tekniska säkerhetsåtgärder som bör tas är bland annat att använda sig utav tvåfaktorsautentisering vilket innebär att man använder sig utav ett lösenord och en sekundär kod eller autentisering för att logga in, olika lösenord till olika plattformar, ha senaste uppdateringen av operativsystem och programvaror samt antivirusprogram. Antivirusprogram hjälper till att identifiera om det finns sårbarheter i en enhet eller fil och skyddar mot bland annat malware och andra typer av virus och intrång. Som komplettering bör man även säkerhetskopiera regelbundet för att skydda mot förlust av data ifall en cyberattack sker eller om en malware krypterar filen och kräver ett lösenord för att återställa åtkomsten till data (Erbschloe, 2019).

Genom att utbilda om cyberrisker och både tekniska och icke-tekniska skyddsåtgärder kan man se till att användare är mer medvetna och försiktiga vid användning av digitala verktyg. Detta kommer således att minska risken för att bli ett offer för cyberattacker. ENISA, Europeiska unionens byrå för nät- och informationssäkerhet, har som mål att säkerställa hög nivå av cybersäkerhet i EU:s medlemsländer. Idag bedriver de forskning och kampanjer för att öka EU:s medborgares cybersäkerhetsmedvetenhet, de anser att detta är en metod för att motarbeta cyberattacker[1].

Alharbi & Tassaddiq (2021), Alqahtani (2022), Aldawood & Skinner (2018) och Shukla m.fl.(2022) rekommenderar att utbildning och införandet av kampanjer i institutioner samt via sociala medier är effektiva metoder att nå ut till studenter och andra användare för att sprida kunskap och ändra attityder gentemot cyberattacker.

3 Metodval

Backman (2016) skriver att det kvalitativa perspektivet innebär hur människan uppfattar och tolkar omvärlden, i kontrast till det naturvetenskapliga tillvägagångssättet som ämnar att mäta något objektivt av verkligheten. I det kvalitativa perspektivet ligger betoningen på hur individen tolkar och upplever en viss företeelse, oftast i ett verklighetsbaserat fall med forskaren som observatör och människan som det observerande. Backman (2016) menar att

[1] ITM8 Konferens om Cybersäkerhet, Göteborg, 24/03/2024.

kvalitativa studier oftast är induktiva till sin natur, vilket innebär att det utifrån empiri & data skapas hypoteser och teorier.

Det finns olika sätt att generera kvalitativa data. Enligt Denscombe (2018) är forskningsintervjuer en metod för att samla data genom människors svar på de frågor forskaren framställt. Fokuset ligger på vad som utförs, vad som sägs, vad de tror sig göra samt deras åsikter. Det är passande att använda intervjuer som metod när syftet är att förstå fenomen såsom: känslor, erfarenheter och åsikter där syftet är att fånga människornas förståelse (Denscombe, 2018). Med detta i åtanke har personliga intervjuer valts som metod eftersom det är relevant och lämpligt då denna studie ämnar fånga in respondenternas uppfattning och åsikt av digitala säkerhetshot samt deras erfarenhet av skyddsåtgärder. Personliga intervjuer spelar en central roll i forskningsmetoden enligt Backman (2016), det används för att förstå individers personliga historier och uppfattningar. Semistrukturerad intervju är en kombination av öppna och stängda frågor, denna blandning av frågetyper möjliggör flexibilitet och struktur och är det som valts för denna studie (Denscombe, 2018). Öppna frågor är en väsentlig del av dessa intervjuer, eftersom de tillåter deltagarna att fritt uttrycka sina funderingar. Detta är av särskilt relevans för att fånga deltagarnas personliga uppfattningar och berättelser, vilket är en aspekt som är central vid kvalitativa metoder. Å andra sidan bidrar den strukturerade delen av intervjuerna, i vilket bestämda frågor används, till att säkerställa att relevanta ämnen täcks.

Denna studie utfördes utifrån ett kvalitativt perspektiv. Detta har motiverats utifrån olika faktorer. Många av de tidigare studierna från litteraturgranskningen har fokuserat på studenters medvetenhet av informationssäkerhet men de flesta har varit av kvantitativt inslag. För att förstå cybersäkerhetsmedvenhetenen bland studenter och deras beteenden bör vi först förstå bakgrunden till deras beteenden och identifiera riskbeteenden samt tankemönster. Vi har därmed valt en kvalitativ metod med semi-strukturerade intervjuer för att besvara frågeställningen med djupgående empiriska data. Totalt har 9 respondenter intervjuats. Denna låga antalet deltagare kan påverka generaliserbarheten av studien. Dock så är syftet med en kvalitativ metod att få en djupare förståelse snarare än att generalisera fynd till en bredare population. Denna ansats har därmed valts för att den passar bäst med studiens syfte.

3.1 Litteraturinsamling

Backman (2016) förklarar att det är genom litteraturgranskningen sammanhanget och vetenskaplig kunskap kan återfinnas genom begrepp, metodik, relevansen, och de kunskapsluckor som finns inom ett givet ämne.

Vetenskapliga artiklar om tidigare forskning har samlats in genom att använda olika databaser som Business Source Ultimate, IEEE och Scopus. Kriterierna för de alla vetenskapliga artiklar som valts är att de varit vetenskapligt granskade, publikation under 2000 - talet samt dess relevans till studien. Den ena författaren läste vid varje sökning ca 5-15 abstrakt, efter det valdes de artiklar med mest relevans till studien. Vissa artiklar hittades genom kedje-sökning via de valda vetenskapliga artiklarna. Den andra författaren läste ett flertal titlar där studier med återspeglande titel för syftet av denna studie blev av intresse, varpå ett mindre antal

abstrakt lästes för att avgöra dess relevans. Således valdes de artiklarna med mest relevans för denna studie genom att avgränsa till titlar och abstrakt som återspeglar denna studie.

Under intervjuerna framgick det att några respondenter använder sig av VPN för att skydda sig online. Av denna anledning har det sökts artiklar som förklarar VPN och dess koppling till IT säkerhet. VPN har även använts som nyckelord inom sökningen eftersom övriga artiklar regelbundet nämnde VPN utan att skriva funktionen och syftet av VPN.

En granskning av de senaste nationella rapporterna gjordes genom Googles sökmotor. Genom den sökningen hittades ENISAs rapporter om de största hoten. För att förstå definitionen av de olika huvudbegrppen kopplade till studien som bland annat ”Cybersäkerhet” och ”Informationssäkerhet” valdes definitionerna ifrån FN och ISO som är en internationell standardiseringsorganisation som utarbetar standarder för experter och näringslivet världen över. Dessa rapporter innehåll information om flera IT attacker vilket är varför sökningar efter enskilda IT attacker inte utfördes.

Söktermer	**Sökträffar**	**Kriterium**	**Databas**
Cybersecurity awareness OR “information security” OR” cybersecurity awareness” OR” information secuirty awareness” AND Student OR “pupil*” OR ”undergraduate” AND “university” OR ”college” OR ”higher education”	66	Vetenskapligt granskad (2014- 2024)	Business Source Ultimate
VPN OR Virtual Private network AND benefit* OR” use”, OR ”advantage”	73	Vetenskapligt granskad (2014- 2024)	Business Source Ultimate
”Cyber attack*” OR ”Network intrusion” OR Malware attack* OR “Cyber terrorism” AND Economic Impact, OR “Financial Loss*”, OR Social Implication* OR “Legal consequence”, OR Ethic* OR “Digital Right* OR “International law”	133	Vetenskapligt granskad (2014- 2024)	Business Source Ultimate
Cyber AND Cybersecurity AND security awareness	221	Vetenskapligt granskad	Scopus
Cyber AND Cybersecurity AND security awareness AND Student	57	Vetenskapligt granskad	Scopus

Cyber AND Cybersecurity AND security awareness AND Student	74	Vetenskapligt granskad	IEEE

3.2 Urval & procedur

För studiens syfte har ett explorativt urval med subjektiv urvalsprocess tagits. Denscombe (2018) skriver att explorativa urval förknippas med småskaliga forskningsprojekt och kvalitativt data. Syftet av ett explorativt urval skrivs vara att generera insikter inom ämnet. Vidare skriver Denscombe (2018) att det finns olika tillvägagångsätt att göra urval som kan åstadkomma ett explorativt urval. Det icke-sannolikhetsurvalet är ett exempel på detta som innebär att forskarna har valfrihet under urvalsprocessen.

Denscombe skriver (2018) om olika tekniker för icke-sannolikhetsurval. Ett av dessa är det subjektiva urvalet vilket innebär att fokusera på en liten mängd personer som har valts ut på grund av särskilda egenskaper såsom relevans och erfarenheter. Det subjektiva urvalet kan väljas när en forskare redan besitter kännedom inom området som ska undersökas och väljer de ting som tros generera mest värdefulla data. Genom att välja en subjektiv urvalsprocess tillsammans med ett explorativt urval, förses forskaren med kvalitativ information och värdefulla insikter. Därmed har studenter inom IT och datavetenskap valts, och går hand i hand med vad Denscombe (2018) menar är lämpligt genom att utföra ett subjektivt urval. Urvalet av studenterna från de olika institutionerna baseras på deras tillgänglighet och målet att uppnå en akademisk spridning.

3.3 Datainsamling

Intervjufrågorna formulerades dels genom inspiration från litteraturgranskningen som återfinns under teoretiska referensramen och med hjälp av AI. Intervjuguiden var semistrukturerad med en klar uppdelning av start, början och slut med förutbestämda huvud och improviserade följdfrågor. Med intervjuguiden skapades en atmosfär där förhoppningen var att deltagarna skulle känna sig bekväma för att dela med sig ärliga och detaljerade erfarenheter.

3.4 Genomförandet

Sammanlagt intervjuades 9 studenter. Fyra respondenter blev intervjuade digitalt samt fick information om syftet skriftligt eftersom de var lokaliserade i olika städer, resterande fem respondenter fick information på plats. Under första intervjun skickades inte frågorna i förhand till respondenten. I efterhand insåg ena författaren att det hade varit effektivare att skicka frågorna så att respondenten kunde få tid till att förbereda sig samt att vissa av frågorna krävde förtydligande. Intervjun var därmed en iterativ process som utvecklades vidare för ena författaren. De efterkommande respondenter fick ta del av intervjufrågorna i förhand för att förbereda sig. Detta skapade en tydlig skillnad på kvalitén av data eftersom intervjuerna blev enklare att utföra då respondenterna hade förberett sig iförhand med sina insikter och kunde enklare svara på eventuella följdfrågor. Intervjun med dessa fyra utfördes digitalt via

videosamtal och spelades in. Respondenterna blev informerade om forskningens syfte, hur data skulle behandlas och gav samtycke för inspelning och lagring av data. Övriga fem respondenter intervjuades av den andra författaren som befann sig i samma stad och plats som respondenterna. Intervjuerna utfördes fysiskt och respondenterna informerades om hur data skulle behandlas, syftet med intervjun och gav samtycke för inspelning och lagring av data. Intervjuerna spelades in och samtliga intervjuer blev transkriberade, anonymiserades samt analyserades utifrån principerna för tematisk analys.

3.5 Tematisk analys

För att utföra dataanalys har vi använt oss av tematisk analys som tillvägagångsätt. Braun & Clarke (2006) skriver att tematisk analys inom kvalitativa studier är en metod för att identifiera, analysera och rapportera mönster inom data. Braun & Clarke (2006) menar att tematisk analys består av ett antal faser:

- Att bekanta sig med sin data.
- Att generera koder utifrån sin data vilket innebär analytiskt arbete genom att data organiseras inom grupper.
- Att söka efter teman genom att koder sorteras till potential teman. Inom detta steg kan forskaren få en översikt kring hur olika koder formar ett övergripande tema.
- Att bearbeta teman.
- Att definiera teman. Under denna fas utförs analyser för varje enskilt tema.
- Att skriva rapporten med färdiga teman. Denna fas innebär att övertyga läsaren genom en sammanhängande text med dataexempel.

I denna studie utförde vi den tematiska analysen genom att genomföra en öppen kodning på varje enskild transkribering av intervjuerna. Att noggrant koda varje enskild transkriberingen gav oss möjligheten att bekanta oss med studiens data på ett djupare plan samt identifiera mönster och teman. Det som kodades under den öppna kodningen var data som var relevant för studien. Efter denna process utfördes en axiell kodning där varje kod från den öppna kodningen placerades inom kategorier och blev tilldelad en färg. Alla kategorier och teman med relevanta citat från transkriberingarna visualiserades därefter i Miro för att få en övergripande bild och enklare visualisera samband.

Alla kategorier sammanställdes sedan i ett separat Word dokument där de placerades utifrån olika färgade teman som identifierades, vilket visas i figuren nedan. Exempel på processen som helhet som har varit exempelvis varit koder som handlade om pengar i olika sammanhang som slutligen tillhörde temat ”ekonomiska aspekter”. Teman i det separata dokumentet analyserades för att generera hypoteser, samband och insikter, vilket är i likhet med det Backman (2016) kallar induktion. Resultat, analys och diskussions avsnitten sammanställdes utifrån forskningsfrågorna, tematiska analysen och den teoretiska referensramen som grund. Därmed kunde paralleller dras mellan teman och den teoretiska referensramen genom att underrubrikerna speglar dess innehåll.

Nedan visas exempel på färgkodningen och teman som identifierades:

Bakgrund & utbildning	
Formativa erfarenheter	
Kunskap om IT-säkerhet & kunskapskällor	
Erfarenhet av attacker	
Attityder och känslor	
Brister i IT-säkerhet och riskbeteenden	
Vidtagna skyddsåtgärder	
Ekonomiska aspekter	
Egna rekommendationer och önskemål	
Värderingen av data	
Förebyggande automationsprocesser	

3.6 Etik

Denscombe (2018) skriver om forskningsetik. Dencombe (2018) menar att det är forskaren själv som måste ta personligt ansvar över sina handlingar under ett forskningsprojekt. Till hjälp åt detta finns det forskningsetiska koder som upprättar huvudprinciper som kan fungera som en moralisk kompass för forskning.

Denscombe (2018) nämner följande 4 etiska huvudprinciper:

1. *Deltagarnas intressen ska skyddas*. Det måste försäkras att deltagarna inte lider av fysiska, psykologiska eller personliga skador som en följd av forskningen.
2. *Deltagandet ska vara frivilligt och baserat på informerat samtycke*. Deltagarna måste förses med tillräcklig information för att göra utföra ett väl genomtänkt om de vill delta eller inte. Denscombe (2018) skriver att samtycket måste vara skriftligt, men om detta inte går att följa ska det finnas ett underförstått samtycke.
3. *Forskare ska arbeta öppet och ärligt i relation till undersökningen*. Forskarna förväntas vara ärliga med studiens syfte och vara tydliga med vilken roll som deltagarna kommer att ha inom forskningen.
4. *Forskningen ska följa den nationella lagstiftningen*. Forskningen måste vara inom ramen för de gränser som kan klassas som godtagbara forskningsämnen. Dataskyddslagar ingår även inom den nationella lagstiftningen.

   Vetenskapsrådet (2017) skriver om forskningsetik och forskaretik i deras rapport. Vetenskapsrådet (2017) förklarar att forskningsetik avser etiska överväganden med hänsyn till de som medverkar i forskningen medans forskaretik avser forskarens ansvar i relation till forskningen. Att forskaren känner till lagstiftningens betydelse för det vetenskapliga arbetet är ett viktigt ansvar. Vidare skriver vetenskapsrådet (2017) att forskarens kännedom för olika lagar och riktlinjer skiljer sig åt beroende på forskningens natur. Av denna anledning listas några av de lagar och riktlinjer vetenskapsrådet (2017) nämner som är relvant denna studies natur:

Personuppgiftsbehandling – Åt personuppgifter räknas det som direkt eller indirekt kan knytas till en person. Behandling av dessa, i synnerhet känsliga personuppgifter och uppgifter kring lagöverträdelser kan kräva tillstånd från en etikprövningsnämnd.
Etikprövningslagen – Lagens syfte är att skydda människan i fråga och att visa hänsyn till människovärdet vid forskning.

För denna studie har etiska principer varit högt beaktande och vägledande under både intervjuprocessen samt hanteringen av data. Alla intervjuer inleddes med en kort introduktion av arbetet och vad studien har för mål och syfte. Det förklarades att intervjun skulle spelas in och deras muntliga samtycke efterfrågades (princip 2 & 3). Alla intervjupersoner informerades om att de närsomhelst kunde avbryta inspelningen och att deras identitet skulle anonymiseras under dataanalysen. Vetenskapsrådet (2017) skriver att helsingforsdeklerationen betonar att forskaren skall säkerställa försökspersonernas rätt till personlig integritet och ”skydd mot insyn i sitt privatliv”. Detta har vi följt genom att benämna samtliga intervjupersoner med ett feminint pronomen som ”hon” eller ”henne”. Intervjuguiden var semi-strukturerad för att möjliggöra ett öppet samtal. Vi informerade deltagarna om att inspelningen kunde avbrytas närsomhelst för att garantera och prioritera deras välmående ifall intervjuguiden hade väckt obehag. Det garanterades även att inspelningarna inte skulle spridas vidare utöver oss (princip 1, 2 & 4). Intervjuerna avslutades med ett tack för deras deltagande och en kommentar om deras svar är värdefulla för forskningsresultaten. Slutligen gavs en uppmaning om att de alltid kunde kontakta oss om några funderingar skulle dyka upp. På detta sätt observerades huvudprinciperna 1–4.

Observerandet av de etiska aspekterna har varit en relativ enkel utmaning. Detta kan bero på att studien inte är omfattande vad gäller intervjufrågornas natur men även antalet respondenter som valde att svara på frågorna. Intervjufrågorna var exempelvis inte utformade på ett sätt där mycket känsliga uppgifter skulle vara förekommande utan handlade istället om mindre känsliga erfarenheter och uppfattningar. Detta, tillsammans med det faktum att respondenternas muntliga samtycke efterfrågades bidrog möjligtvis till att en etikprövning inte behövde utföras dels på grund av frågornas omfång och dels då studien är av en mindre skala. Detta gjorde processen mycket smidigare och gav oss möjligheten att istället utföra intervjuerna väl förberett med huvudprinciperna ständigt i åtanke, vilket var enkelt att följa. Att fokusera på huvudprinciperna som vägledande etiska principer gav oss ovärderliga insikter av att bedriva etisk forskning. Genom att bland annat tydliggöra våra intressen och etiska överväganden skapades en god och positiv dialog mellan oss och respondenterna, vilket vi uppfattade bidrog till att intervjupersonerna kände sig mer öppna och villiga på att tala mer fritt. Denna positiva utkomst gav oss även förståelse och insikt för värdet av ärlighet, respekt och ansvar.

4 Resultat

I denna del av studien kommer resultatet att beskrivas kring hur studenterna uppfattar informationssäkerhet, deras kännedom av olika attacker och deras beteenden i relation till deras kunskap. Dessa aspekter delas in i underkategorier, där deras beteenden sammanfattas.

Underkategorierna speglar forskningsfrågorna och den tematiska analysen. Exempelvis motsvarar underkategorin ”informationssäkerhet” temat ” Kunskap om IT-säkerhet & kunskapskällor”.

4.1 Informationssäkerhet

Samtliga respondenter har utbildningsbakgrund inom IT och datavetenskap vilket kräver daglig uppkoppling till internet och har använt sig av internet sedan barndomen. Respondenterna har visat på en god nivå av medvetenhet och förståelse för informationssäkerhet. För de allra flesta respondenter innebär informationssäkerhet att skydda ens dator och uppgifter från obehöriga användare.

Respondent 5 svarar på följande omfattande vis:

” jag tänker på är att ett system som blockerar. Blockerar en obehörig individ. Det är det första jag tänker på och det andra jag tänker på är att hur vi ska säkerställa själva processen för att se till att inget av det sker” - Respondent 5

Liknande svar gavs av respondent 3. Respondent 2 visade på liknande medvetenhet men visade på mer teknisk förståelse av attacker för hennes svar. Respondent 2 svarar på följande vis:

”Det är väl konto som blir snodd eller känslig information som blir snott på nätet. Bedrägeri och liknande som hänt väldigt ofta rent generellt... Om man har sparat sitt kort någonstans och sen den hemsidan eller den appen blir hackad så förlorar man.” – Respondent 2

Respondent 4 följer på samma spår men kopplar det kring nätverk och attacker som kan uppstår inom det:

”Jag tänker på, alltså jag tänker på lösenordet fältet när bokstäverna visas som stjärnor även med wifi och WiFi manager. Jag tror säkerhet brukar gälla konto, dina personliga konto som annars skulle kunna hackas av någon annan ” – Respondent 4

Den sista meningen reflekterar återigen en medvetenhet om att informationssäkerhet handlar om att skydda ens dator från obehöriga. Respondent 8 visar i likhet med detta en medvetenhet om flera olika typer av attacker och en hög riskmedvetenhet om att man aldrig kan vara helt säker på nätet. Hon visar även en oro för risken att information läcker ut.

”man ska vara säker så mycket som det går för att det är ganska mycket information som kan läcka ut från din dator och från dina när du betalar för olika grejer. Det är ganska mycket data och information som kan läggas ut som ska vara så mycket som möjligt, men samtidigt så är det ganska svårt att vara 100 % säker. Eller egentligen, det är omöjligt att vara 100 % säker. Det ena är att stänga av internet då.” – Respondent 8

Vidare förklarar respondent 8 att hon vill lära sig mer om IT-säkerhet för att kunna skapa säkra system och webbsidor. Hon föredrar att lära sig från erfarna seniorer inom branschen.

”Såklart kommer lära mig mycket mer om IT säkerhet för att om jag ska koda i framtiden och om jag ska lära mig om hur man ska säkra olika typer av hemsidor och system som jag kommer att skapa då behövs en kunskap av hur dessa attacker sker. Först och främst är det kanske via seniorer, för att man får erfarenhet från andra när man jobbar på olika arbetsställen” – Respondent 8

Respondent 9 visar även på viljan att lära sig mer och är införstådd på att hon kan vara sårbar. Vidare förklarar hon varför hon vill lära sig mer.

”jag tror att det finns en massa saker som jag inte känner till. Och då är jag säkert i de här fällorna och är sårbar…Jag hade velat lära mig mest för att jag tror att det kommer att bli värre… och det kan man ha möjlighet att googla men det hade ju varit ganska snyggt att få det i något format. Att ‘det här är det vanligaste attackerna i Sverige som händer privatpersoner eller företag. Och det finns enkla sätt för att skydda sig mot sådant. ´” – Respondent 9

Respondent 1 tänker mer kring mjukvara och verktyg:

”program som på något sätt gör det alltså säkrare för dig då att använda antingen internet. Ja det var det var jag skulle alltså tro något slags antivirusprogram eller kanske något annat. Alltså det finns så många olika, alltså olika säkerhetsmöjligheter Från antivirus till third party grejer på internet och det finns jättemånga”

Respondent 7 är medveten om riskerna med IT-attacker men uttryckte att hon inte visste hur man kunde implementera effektiva säkerhetsåtgärder. Respondent 7 visade även en medvetenhet om att angripare ständigt utvecklar nya sätt att attackera och att metoderna snabbt utvecklas. Liknande medvetenhet uttrycker respondent 6.

”Det är viktigt att skydda sig själv och skydda olika system och så. Men jag är inte insatt i hur det funkar och hur man skyddar. Om man säger alltså jag bara hört om det.”- Respondent 6

Respondent 7 visar grundläggande förståelse för informationssäkerhet men tror sig inte utgöra en attraktiv måltavla för angripare. Respondent 1 hade samma uppfattning innan hon utsattes för hennes första intrång. Respondent 6 beskriver på liknande spår och uttrycker en viss immunitet mot att bli utsatt av attacker med tanke på att hon inte upplevt något sådant tidigare.

“Jag känner så här...ibland är jag inte så där jätteviktig person så att det är ingen som skulle vara direkt intresserad av att komma och hacka mig. Men jag kan tänka mig, om man är mer känd så borde man vara mer försiktig.” - Respondent 7

4.2 Kännedom av attacker

Under denna rubrik visas resultatet kopplat till teman ”Erfarenhet av attacker”, ”formativa erfarenheter” och ”kunskap om IT-säkerhet och kunskapskällor”. Eftersom vissa data från de identifierade teman överlappar har därmed mer djupgående data från temat ”kunskap om IT-

säkerhet och kunskapskällor” även redovisats i denna rubrik och föregående rubrik.

Respondenterna har visat på en god kännedom av olika IT attacker. Kännedomen har uppstått antingen genom egna erfarenheter av IT attacker, socialt umgänge, utbildning och nyheter samt genom spelvärlden. De mest igenkända attackerna var intrång, phishing och social engineering.

4.2.1 Erfarenhet av IT-attack

Respondent 8 har tidigare blivit utsatt för ett lyckat intrångsförsök på ett av hennes e-postkonton, men som enligt henne inte innehöll värdefulla data. Respondent 1 återger liknande personlig erfarenhet av försök till intrång men som utfördes på flera av hennes personliga konton, varav 1 attack lyckades:

”... som tur är så får man ett mejl direkt då när det här alltså sker så kan man gå in och ändra. Men ibland är det för sent och det har alltså skett exempelvis att en person har gått in på mitt email account och raderat alla alla mejl alltså. Som tur är så använder jag nu twofactorautentictication på allting bara.” – Respondent 1

Dessa intrång bidrog till båda respondenter att vidta säkerhetsåtgärder framöver.

“Intervjuare: den här attacken som du utsattes för, hur känner du att den påverkade din uppfattning av IT säkerhet?
Respondent: ...att ibland på olika sätt skapa verifikation eller verifiera det med mobilen så att du har extra säkerhet.... Så det är kanske det som motiverade mig att ha det i mina nuvarande konton” - Respondent 8

Respondent 3 återger när en av hennes vänner blev utsatt för en IT attack vilket öppnade upp hennes ögon och fick henne bli mer seriös av IT säkerhet:

” Ja, jag känner igen min kompis...Någon hade hackat hans Facebook. Så det de hade gjort var att de skickade länken till honom. Sen länken går han in på och skrev sin inloggning. Sen efter några timmar hans kontot, de tog över den och sen använder hackaren använda min kompis konto... Nu jag började liksom alltid kolla och inte gå efter om någon skickar till mig länkar och sånt.”

Respondent 6 var med om ett intrång försök som en följd av att hennes pojkvän hade av misstag öppnat port-forwarding-gate i deras Raspberry Pi. Hackaren försökte utvinna hennes pappas kryptovalutor.
Respondent 5 har även en personlig erfarenhet från hennes tidigare år när hon laddade ner virusrelaterade innehåll på hennes Samsung mobil vilket fick henne bli mer seriös kring IT attacker:

” Jag fick lära mig den hårda vägen att inte ladda ner vilka filer som helst och att använda VPN i vissa scenarior och allt möjligt. Att skydda sig för sådana. ” - Respondent 5

Spelvärlden har även varit en bidragande faktor till att förstå olika typer av IT attacker. Respondenter 2 och 4 har blivit introducerade till olika IT attacker genom spelvärlden från tidig ålder där begrepp som DDOS, IP attacker och trojanska hästar varit förekommande. Respondent 3 har även blivit utsatt för virus när hon laddade ner ett gratis spel. Respondent 4 återger:

" Jag brukade spela ett spel och i spelet alltså du kan sälja saker för pengar i verklighet. Så ibland handlar det om ganska mycket pengar. Du vet alltså 5000 kr, 10 000 tusen kr. Så jag menar, om någon riskerade 10 000, om någon blev av med pengarna, jag har hört talas om att de blivit DDOS attackerade." - Respondent 4

För flera av studenterna har nyheterna och online artiklar spelat en roll i att öka förståelsen om olika attacker. Respondent 8 förklarar att hennes kunskapskälla är en blandning av hennes formella akademiska utbildning men även mycket från nyheterna, som har väckt hennes nyfikenhet att lära sig mer:

"...Något händer och man tänker. Vad hände här? Typ att en sida gick ner. Varför händer det? Varför påverkar en attack eller Facebooks hemsida att de förlorar mycket pengar på det? Det är ganska intressant information som man kanske läste på lite i under sin egentid." - Respondent 8

Liknande svar återger respondent 3 som nämner att hon har hört talas om att Sony blivit utsatt för IT attacker vilket hon läst om på nyheterna. Hon återger även att hon numera regelbundet läser online tidningen "Computer Sweden". Respondent 7 säger att hennes nuvarande kunskap om IT-säkerhet är från olika online källor.

"dels är det på internet man ser mycket och i mina studier jobbar vi mycket med internet. Man ska kolla upp saker. Man ska programmera olika system och då måste man veta lite om det här är säkert, tex att lägga dessa privata adresser ute hur som helst. De måste ju skyddas, så att säga. Så dels i universitetet, dels på internet, dels vänner man pratar med och det man ser på nyheter" – respondent 7

4.2.2 Social engineering

Att äldre personer ofta manipuleras genom social engineering var även välkänt bland respondenterna, där källan till denna medvetenhet oftast var nyheter. Respondent 5 och respondent 7 sammanfattar denna kollektiva medvetenhet:

" Man läser ju överallt att fler äldre blir hackade och det är mycket bedrägeri när det kommer till att skicka vissa typer av meddelande som frågar om ens bankuppgifter och så vidare eller liknande uppgifter generellt " - Respondent 5

"...jag tycker man borde hålla workshops speciellt för äldre, för det är de som brukar drabbas mest av just cyberattacker eller i alla fall nätfiske." - Respondent 7

Alla respondenter känner igen attackerna phishing och olika sammanhang av social engineering. Falsk reklam visar sig vara enkelt att identifiera för flera respondenter baserat på hur själva reklamen är utformat designmässigt och de finansiella löftena avslöjar direkt att det inte är legitimt medan för länkar menar respondenterna att de ofta analyserar de.

Respondent 3 återger att hon tidigare har utsatts för bedrägeriförsök men enkelt identifierar situationen. Dessutom återger hon att hennes mobil automatiskt hanterar sådana försök:

”… Min mobil nu hanterar direkt automatiskt om den är scam… De flesta hemsidor har reklam men de jag misstänker alltid har lite speciell reklam, liksom de kräver att du ska göra så och så. Jag känner igen att den där hemsidan har virus... Att personen liksom ger dig enkla tips att du kan tjäna pengar. Och säga till exempel att om du gör så, du kan jobba på distans och du kan tjäna såhär mycket pengar. Det är omöjligt. Jag känner direkt att den är scam.” - Respondent 3

4.2.3 Phishing attack

Majoriteten av respondenterna var vaksamma om phishing attacker. Respondent 4 sammanfattar olika phishing tekniker och vad som oftast avslöjar phishing, Respondent 8 formulerar sig på ett liknande sätt.

”Det kan handla om pengar till exempel. Jag har 1 000 dollar för dig, men du behöver bara ge mig den här informationen så jag kan skicka till dig. Till exempel, det kan vara någon som de lovar dig pengar för att få din information nu. Nu oftast är det finns folk som använder bilder av kvinnor och de säger jag vill vara med dig och jag vill träffa dig och det är jättepopulärt, men det är jätteenkelt att säga att den är falsk” - Respondent 4

Respondent 7 nämner att hon upplever phishing försök nästan varje dag via e-post och SMS, hon har lärt sig att identifiera och undvika det.

”Respondent 7: Nästan varje dag blir jag kontaktat av någon.
Intervjuare: hur hanterar du den situationen?
Respondent 7: Oftast hamnar de på skräpinkorgen direkt. När jag går in där så ser jag att nästan varje dag eller typ någon gång i veckan så försöker någon skicka mejl eller SMS. Jag brukar inte klicka på dom.”

När respondent 6 tillfrågas hur hon kan identifiera ett phishing försök uttrycker hon sig på ett liknande sätt som de andra respondenterna, men där hon tillägger att hon använder sig av rimlighets analys och känslor:
“Typ att det kommer en länk från någon oväntat. Det känns redan då som att det är lite red flag, för att det känns som att om jag får en länk som jag ska klicka på så är det ofta från någon jag känner och det finns en ganska rimlig kontext för det. Det är sällan de skriver bara ´Klicka på det här eller det här´. Eller att någon på Facebook som man inte har pratat med på liksom 5 år säger sånt.... Då känns det ganska uppenbart att det här är inte du som skriver det här till mig. Så det kanske är mer rimlighet analys på något sätt.” – Respondent 6

4.3 Beteenden

Under denna rubrik visas resultatet för teman ”brister i IT-säkerhet och riskbeteenden”, ”vidtagna skyddsåtgärder”, ”attityder och känslor” samt ” värdering av data”.

Majoriteten av respondenterna visade på goda säkerhetsrutiner inom underkategorierna user vigilans, lösenordshantering och programvaror. Majoriteten av respondenterna uppvisar försiktighet med länkar, känner igen när e-mail och sms visar på lustiga tecken som tyder på skadlig kod.

4.3.1 User vigilans

En majoritet av respondenter uppger försiktighet och analytiskt beteende online. Detta rör sig först och främst kring programvaror, länkar, e-mails och sms. 4 respondenter uppger försiktighet med att inte ladda ner vilka filer som helst och att de inte trycker inte på misstänksamma länkar. Respondent 9 visar försiktighet när hon klickar på länkar som verkar misstänksamma, hon undviker även att kopiera webbadresser direkt. I stället navigerar hon till källans huvudsida och klickar sig fram till den hänvisade sidan.

Respondent 2 och respondent 7 berättar att de brukade få sms som påstod sig vara från postnord och ville ha deras personnummer men förstod dels att det var falskt eftersom de inte beställde något, dels genom att analysera hur postnords faktiska hemsida och design såg ut jämfört hemsidan till den länken de fick. Liknande åtgärder beskriver respondent 5. Respondent 4 återger att extra försiktighet efterföljs om hon ansluter sig till offentliga nätverk och får även varningsmeddelanden från hennes operativsystem som bekräftelse för att bejaka extra vaksamhet. Respondent 2 uppger att hon inte alls använder sig av offentliga nätverk utan sin mobildata.

”…Till exempel om jag kopplar till en offentlig public network, Jag kommer inte logga in på mina, alltså mitt email, personlig email och vissa personliga saker…Jag kommer vara försiktig att inte spara mitt lösenord och inte utnyttja datorn om den inte är min. ”- Respondent 4

4.3.2 Programvaror och nedladdning

Försiktighet är förekommande bland en majoritet av respondenterna innan nedladdning av vissa programvaror. Det handlar om att undersöka källan bakom de som utvecklat programvaran eller att nedladdningssidan är pålitlig. Respondent 3 berättar om hennes rutin:

” …Speciellt när jag laddar ner vissa verktyg som jag använder. Jag kollar om de är äkta och inte liksom scam liksom. Så jag alltid kollar liksom med hur, alltså jag kollar hemsidorna som är riktiga som jag laddar ner från liksom. ” – Respondent 3

Liknande åtgärd beskrivs av respondent 5 som lägger till trustpilot som hon använder sig av för att kontrollera validiteten av något:

” … Jag vet att jag inte ska ladda ner vissa typer av filer, att jag inte ska öppna vissa typer av mejl eller trycka på vissa typer av länkar som jag får… Jag går in på Trustpilot eller går in på liknande källor för att dubbelkolla och vara källkritisk nog för att veta om den är trovärdig eller inte.”

Respondent 8 beskriver att han är försiktig och ser till att nedladdningen är från företagets ursprungliga plattform och att URL:en har krypteringen “HTTP:S":

“Först när man söker på webbläsaren är det första viktigaste kanske att det inte ska stå “http” och det ska stå i stället “https”. Det ska finnas ett S på slutet… Men sen även kanske att inte ladda ner från kanske företag som man inte känner till. Något som jag tycker låter relevant är att kolla om det här är rätt webbsida. Att det inte är en fake webbsida” - Respondent 8

Däremot nämner en respondent att de inte vidtar försiktighetsåtgärder för att kontrollera pålitligheten av olika programvaror utan förlitar sig på systemens inbyggda säkerhetssystem samt på omdömet av hennes universitetslärare om hon blir tillsagd att ladda ner mjukvara.

“Med vissa saker så skulle jag säga att jag bara laddar ner och inte tänker så mycket på det. Jag tror att nu för tiden så känns det som att det mesta jag laddar ner är inom någon kurs.…Och då litar man kanske på det för att man har fått det rekommenderat av typ en lärare eller så... jag har Mac och om det kommer via app-store så känns det som att jag litar på det och då tänker jag inte mer på det” - Respondent 6

Respondent 6, 7, 8 och 9 säger att de uppdaterar programvarorna så fort de får en påminnelse.

”Jag brukar nog göra det på rekommendation av datorn. Det är nog bara det faktiskt. Jag söker nog sällan upp själv.” – Respondent 9

Respondent 6 och respondent 9 förklarar att de är mer måna om att numera uppdatera programvara och operativsystem oftare efter påbörjad IT utbildning, där de lärde sig att man kan motarbeta hackare med senaste uppdateringen.

”…relativt snabbt. Och det är lite för att speciellt efter jag läst den här kursen om etisk hackning så märkte man att det är specifikt den här versionen man behöver…Då märkte man att om man hänger med och uppdaterar, då kommer man ju kanske förhoppningsvis hinna ifrån de där … Att man liksom inte är kvar på något gammalt där de har hittat någonting.” – Respondent 6

”Innan skulle jag se att det fanns en uppdatering, men jag tänkte nog inte på vad en uppdatering var liksom. Nu tänker jag att det är lika bra att uppdatera på en gång för att de kan ha hittat fel eller förbättrat något. Så den tanken har jag nog mer nu efter utbildningen.” - Respondent 9

Att använda sig av VPN för att säkerställa säkerhet online är förekommande bland 3 respondenter. Respondent 1 menar att hon inte anser att VPN vara tillräckligt säkert medan respondent 2 använder sig av VPN dels av säkerhetsskäl, men började initialt använda VPN för att få tillgång till blockerade spel. Liknande tendens återger respondent 4 som använder sig av VPN men använder det specifikt för att komma åt geo blockerat innehåll och inte av säkerhetsskäl:

" ...Jag använder VPN för att se kanadensiska serier... Jag använder den inte som säkerhet skydd " -Respondent 4

4.3.3 Lösenordshantering

Lösenordshanterandet bland respondenterna skiljde sig åt men lutar mot säkra beteenden för alla respondenter vad avser säkerhetsaspekter som tvåfaktorsautentisering eller styrkan av lösenord. De flesta av respondenterna använder sig av 10 – 15 tecken i sina lösenord och mixar mellan versaler och gemener samt olika tecken och använder sig av tvåfaktorautentisering för att säkerställa ytterligare skydd, men hur ofta detta används och inom vilka tjänster varierar bland användarna. Endast 1 av respondenterna uppgav att hon uppdaterar sina lösenord regelbundet.

Respondent 6 förklarar hennes motiv till noggrann lösenordshantering:
" ...det är för att det var någonting som man fick höra mycket att man ska ha olika lösenord, man ska ha långa allt. Du vet, allt det där. Att det liksom nästan bankars in. Att det var viktigt. Och då tog jag väl till mig det och ´bra och det ska jag göra´.... det är nog lite det att det liksom kom tidigare, att det satte sig på ett annat sätt." - Respondent 6

Respondent 2 och 5 använder sig av olika lösenord på olika tjänster och uppger att de använder sig av tvåfaktorsautentiseringen på allt. Däremot använder respondent 8 och respondent 7 endast tvåfaktorautentisering på plattformar som de anser ha värdefulla data, eller om de blir tvingade till det av plattformen. Respondent 9 använder tvåfaktorsautentisering på plattformar där hon blir uppmanad till det och förklarar även att denna påminnelse ökar hennes förtroende till plattformen.

Respondent 1 och 3 medger att de använder kortare och enklare lösenord för tjänster med mindre känsliga data och som kräver regelbunden inloggning. Lösenorden brukar se det samma ut för dessa tjänster för att hålla det enkelt att logga in. Respondent 1 använder dock tvåfaktorsautentisering för alla tjänster hon använder, även om tjänsterna innehåller mindre känsliga data. Respondent 3 sammanfattar tankeprocessen vilket överensstämmer med övriga respondenter:

"När jag använder mina sociala medier eller personliga konton används mer säkrare lösenord medan jag i skolinloggningen eller andra grejer... Jag upprepar och det kräver hela tiden inloggningar. Så jag använder ganska enkla lösenord " - Respondent 3

Respondent 4 beskriver hennes lösenordshantering som starkt. Respondent 4 menar att hon endast använder sig av tvåfaktorsautentisering för tjänster där pengar ofta är involverade samt att hon använder sig av lösenord med viss grundstruktur med variationer baserat på den

aktuella tjänsten som lösenordet används inom. Respondenter uttrycker en uppfattning om att detta inte alltid är ett säkert beteende och har tidigare fått varningar från hemsidor om att inte ha namnet av en tjänst på lösenordet:

” Jag behåller ett slutet av det här lösenordet och när jag skapar ett konto till exempel på Netflix, jag kallar den stor bokstav N och sen Netflix och sen jag lägger till den här sista del som är lite komplicerad… Jag har fått varningar… Vissa hemsidor, de tillåter inte att ha det” - Respondent 4

Vissa studenter visar på några riskbeteenden. Nedan redovisas de.

Respondent 8 förklarar att hon inte uppdaterar sina lösenord så ofta som hon borde på grund av lathet.

“...Ibland. Man orkar inte byta lösenord varenda månad... Så ja. Men annars skulle säga, jag har kunskapen, men inte att jag använder allt.... Bara lat” - Respondent 8

Respondent 6 förklarar att det är flera studenter som inte vidtar vissa säkerhetsåtgärder på grund av lathet:

“Vi är jättemånga som inte är alltså vana med internet som inte förstår alltså hur enkelt det är att bli hackat...även om även om de här sidorna tvingade typ att ha en stor bokstav och några siffror och allt det här det blir ändå typ att man använder exakt alltså samma eller som på alla sidor och om en sida blir alltså läckt så är det svårt” - Respondent 6

4.3.4 Antivirus

Resultatet visar att 6 respondenter har antivirus nedladdat, varav 3 av dessa har gratis versioner. Resterande 3 respondenter förlitar sig på det förinstallerade antivirusprogrammet inom det operativsystem de använder. 3 respondenter har inget antivirus nedladdat alls.

Majoriteten av respondenter har alltså antivirusprogram men attityderna skiljer sig åt. 3 respondenter använder sig av operativsystemets förinstallerade virusprogram vilket de uttrycker olika uppfattningar och åsikter kring. Hur de gick till väga skiljer sig även åt. Skälen bakom detta är huvudsakligen ekonomiska, förtroendet respondenterna hade på systemet och upplevd lathet.

Studenter med förinstallerade antivirusprogram

” Jag förlitar mig ganska mycket på att mitt operativsystem eller det som kommer med det…Och att saker körs ganska för sig själva. Men det är inget jag funderar speciellt mycket på” – Respondent 6

Orsaken till att Respondent 6 inte medvetet har laddat ner ett antivirusprogram är på grund av irritation. När hon tillfrågas om hon har tänkt på att ladda ner ett antivirusprogram säger hon:

”… de liksom typ hoppar upp och är irriterande och de tar upp mycket. De körs och håller på att sega ner datorn och så. Så det kanske är lite gammal bild av den. Men det är nog lite den bilden jag har och jag känner nog lite att jag inte behöver det. Nej.” - Respondent 6

Respondent 7 beskrev på liknande spår men uttryckte mer osäkerhet kring om hon faktiskt hade antivirus eller inte.

” Jag tror jag har. Jag tror alla datorer har så att man måste ha (skratt).” - Respondent 7

Studenter med gratis antivirusprogram

3 respondenter har gratis versioner vilket de uttrycker olika uppfattningar och åsikter kring. Respondent 4 som numera inte använder sig av ett antivirusprogram beskriver liknande frustration som respondent 6. Respondenten brukade använda sig av ett gratis antivirusprogram men slutade använda det då programmet började kräva prenumeration. Dessutom upplevde hon olika restriktioner på vilket påverkade hennes användarupplevelse:

”… De brukar kosta ganska mycket pengar, abonnemang, och jag tycker inte om att betala för sånt man kunde få gratis innan… Och även de som ingår med dator jag tycker inte om tex den Norton Antivirus, jag tycker inte om den. De bara stör… många notiser och restriktioner, till exempel vissa program när jag installerar dem, de funkar inte. Jag kan inte ladda dem. Det är på grund av den här antivirus” - Respondent 4

Respondent 8 använder sig både av ett gratis antivirusprogram samt det förinstallerade Windows Defender. Respondenten uttrycker ett större förtroende för Windows Defender och en nedsättande syn på hennes gratis antivirusprogram:

”Den heter Avast. Den är 100 % inte bra alls. Det poppar hela tiden. Jag kan betala för att få den fullt premium service för antivirus, men jag klickar alltid på X. Jag litar på Windows Defender mest” - Respondent 8

Respondent 2 beskriver en god kännedom om syftet av antivirusprogram och använder sig av ett gratis antivirusprogram och uttrycker inget negativt eller frustrerande kring det, utan förmedlar en positiv attityd eftersom hon får det gratis tillsammans med hennes VPN:

” Jag nöjer mig med det här. Jag får både VPN och antivirus med det och det har funkat hittills.” - Respondent 2

Studenter utan antivirusprogram

3 studenter har inget antivirusprogram. För respondent 4 är motivet som tidigare nämnt att hon inte vill betala för premiumversioner och tycker inte om antivirusprogram generellt på grund av restriktioner som antivirusprogram orsakar. Respondent 5 känner till konsekvenserna av att inte ha antivirus nedladdat och säger att hennes anledningar främst beror på lathet och ekonomiska anledningar.

Studenter med betalt antivirusprogram

Respondent 9 har ett antivirusprogram nedladdat som hon har köpt. Hon förklarar att hon förstår hur det fungerar någorlunda och uttrycker en känsla av tillfredställelse när programmet bekräftar att hennes dator är skyddad:

"Jag har någonting som heter Clean my Mac som i sig har någon realtime monitoring i datorn och skannar av den hela tiden. Det är typ det jag vet om den eller den kollar igenom filer. Jag kan också aktivt starta en sökning där den kollar igenom filer efter typ skadlig kod eller någonting. Men det är typ så mycket jag vet om den. Jag vet inte mer vad som händer där bakom egentligen, mer än att den säger att du är "protected" och då tänker jag perfekt, då är allt bra, tack. (Skratt)" - Respondent 9

Övrigt om nedladdning

Respondent 6 och 9 laddar ner alla program som lärare har rekommenderat och som finns i app store eftersom de har förtroende för dessa. Då gör de ingen vidare granskning fastän sidan kunde se lite misstänksam ut. Respondent 8 säger också att hon litar på de appar som finns i app store och laddar ner med förtroendet att det bör vara säkert.

4.4 Intresse att lära sig mer

Respondenterna 1,7, 8 och 9 förklarar att de vill lära sig mer och föredrar icke-formella utbildningsmetoder som kampanjer och broschyrer, lärande från erfarna seniorer inom IT, eller evenemang och föreläsningar med lockande motiv. Respondent 7 betonade behovet av engagerande metoder som väcker intresset, för att underlätta kunskapsinhämtningen och utan att det krävs någon form av examination.

Respondenterna 6 och 9 föredrog en formell utbildning inom sin institution, men som borde vara genomgående i olika moment under programmets gång så att det skulle bli enklare att förstå IT-säkerhet i olika kontexter.

5 Analys och diskussion

Vid den tematiska analysen identifierades ett par teman. Under denna del kommer dessa teman att diskuteras och förklaras för att generera insikter kring empirin. Det kommer även diskuteras hur dessa teman hänger ihop med varandra på olika sätt. Varje underrubrik under denna del av arbetet är satt för att reflektera de mest framträdande teman för varje enskild underrubrik, och under dessa diskuteras hur teman hänger ihop. Underrubriken ”relationen mellan kunskap och beteende” omfattas exempelvis av teman ”kunskap om IT säkerhet & kunskapskällor”, ”formativa erfarenheter” och ”attityder och känslor”.

5.1 Relationen mellan kunskap och beteende

Detta stycke presenterar en analys och diskussion om respondenternas kunskap i relation till deras beteende. Vi lyfter även upp de genomgående faktorerna som har påverkat respondenternas kunskap och beteende. Dessa faktorer kan ge oss en förståelse kring hur vissa studenters medvetenhet bidrar till deras beteende.

Studiens empiri har visat att svenska högskolestudenter har en hyfsad nivå av cybersäkerhetsmedvetenhet och beteende vilket skiljer sig från tidigare forskning. Alharbi & Tassadiqs (2021) studie visade att studenter i Saudiarabien brast i cybersäkerhetsmedvetenhet vilket även andra studier även kom fram till såsom studien i Silicon-Valley av Moallem (2019).

Denna studies empiri visar att studenterna känner till grundläggande kunskap om cybersäkerhet, olika typer av IT attacker och skyddsmekanismer. Det må finnas olika orsaker till detta, men kan bottna sig i att Sverige är ett digitaliserat land där många av dagens studenter har växt upp med det digitala närvarande sedan barndomen vilket har skapat erfarenheter, vilket i sin tur lett attityder och förståelse. Exempelvis återger 2 respondenter att online spel som är populära i Sverige blev en introduktion till IT attacker från tidig ålder vilket introducerade de till olika typer av begrepp och säkerhetsskydd, såsom säkrare lösenordshantering och VPN. På liknande spår har något förekommande bland respondenterna varit vad vi kallar formativa erfarenheter av IT attacker vilket höjt cybersäkerhetsmedvetenheten av studenterna. Flera av respondenterna återger någon närstående eller när de själva blev utsatta IT attacker vilket har haft en tydlig koppling till åtgärdande beteenden, vilket även tyder på att cybersäkerhetsmedvetenheten och det uppföljande beteendet inte var lika hög innan de utsattes för en attack. Exempelvis återger en respondent att hon numera använder sig av tvåfaktorsautentisering på alla hennes online konton efter att hon utsattes för intrångsattack. Respondent 1 förklarade att hon inte ansåg sig vara en måltavla för intrångsattacker, men efter attacken ändrades hennes uppfattning och började använda sig av tvåfaktorautentisering. Detta formade både hennes medvetenhet och beteende. I linje med detta antar respondent 7 att även hon inte är en “viktig person” för att utgöra en måltavla för angripare. Riskbeteendet av denna attityd kan återspeglas i hennes beteende av att hon använder sig av enkla lösenord men trots det visar på en aning av cybersäkerhetsmedvetenhet då hon försöker skifta mellan 5 olika lösenord för att öka

säkerheten. En ytterligare sämre medvetenhet reflekteras över hennes uttalande kring osäkerheten ifall hon hade antivirus nedladdat. Denna riskuppfattning kan signalera att deras beteenden kan påverkas av denna attityd, vilket kan leda till mindre försiktighet och sämre tillämpning av säkerhetsåtgärder.

Respondenterna som visade på utövandet av säkerhetsåtgärder visade att det var en följd av antingen erfarenhet av en IT-attack eller på grund av information som införskaffades utanför en formell akademisk utbildning, vilket var via nyheter, sociala medier eller vänner. Flera respondenter har nämligen återgett att de ofta fått höra att äldre oftast blir utsatta för bedrägerier vilket de läst om online. En respondent berättar även att hon i samband med ett intrångsförsök på en närstående till henne började medvetet söka upp nyheter om cybersäkerhet. Detta har visat sig vara en större bidragande källa till medvetenhet bland studenter inom IT och datavetenskap än formell utbildning. Exempelvis sökte många respondenter upp information om IT-attacker online i samband med en attack, vilket respondent 5 gjorde efter att hennes Samsung mobil fick virus.

Attityden till IT framstår av respondenterna generellt vara positiv, vilket Slusky och Partow-Navid (2012) menar är av mer vikt för personers cybersäkerhetsmedvetenhet. En ytterligare förklaring skulle därmed även kunna vara att svenska studenter inom IT och datavetenskap har en positiv syn och vana av informationsteknologi viket möjligtvis förklarar varför vissa respondenter effektiv läser på om cybersäkerhet och implementerar olika åtgärder i samband med en attack. Å andra sidan erkände några av respondenterna att de ansåg att de inte hade tillräckligt med kunskap om cybersäkerhet och ville lära sig mer. Detta visar på en motivation och vilja att utvecklas. Detta går att jämföra med studenterna i Polen som visade på en högre grad av självskattad kunskap i jämförelse med deras faktiska beteende (Oliviera, 2023). En respondent stod ut som uttryckte att han planerar att lära sig mer med syftet att använda det i sin framtida yrkesroll.

Resultatet visar på ett ytterligare formativt beteende. Nämligen att flera av respondenterna kunde identifiera ett phishing meddelande och var försiktiga med att dela sin privata information med obehöriga. Detta var bland annat till följd av deras höga digitala användning och att de med tiden kunde omedvetet särskilja riktiga meddelanden från falsifierade. Detta kopplas till temat formativt beteende vilket visar på att deras beteende har ändrats över tiden och bidragit till deras kunskap, på grund av olika faktorer. Genom att förstå dessa faktorer som påverkar deras beteende kan vi skapa bättre förutsättningar för ett säkert digitalt landskap. Det framstår således att en tidig uppväxt med det digitala, erfarenheterna och lättillgänglig information tillsammans med en positiv attityd till IT möjligtvis bidrar till en ökad cybersäkermedvetenhet.

5.2 Tankar kring lösenordshantering

I detta stycke analyseras och diskuteras respondenternas olika lösenordshantering och faktorerna som bidrar till deras beteende.

Respondenterna har visat på en god lösenordshanteringsprocess tillskillnad från Alharbi & Tassadiqs (2021) studie som visade att studenterna brast inom detta område. En respondent beskriver att detta beror på grund av tidig repetitiv information och påminnelser kring varför det är viktigt med långa lösenord medan för de flesta respondenter har detta berott på tidigare formativa erfarenheter samt det värde som ligger inom ett visst konto. En möjlig förklaring varför studenterna visade god lösenordshantering är således att studenterna korrekt värderar och avgör vad som är viktigare att skydda och mindre viktigare att skydda. Uppfattning kring detta kan variera från person till person men ett upprepande mönster har varit skyddandet av det som innehåller något av ekonomiskt inslag eller känsligdata. Mindre säkrare lösenord användes åt det som antingen inte värderas högt eller som kräver regelbunden inloggning vilket är varför det sätts ett enklare lösenord för att göra upplevelsen smidigare. Värderingstemat kan alltså vara en anledning som påverkar lösenordshanteringen. Respondent 8 reflekterade över detta som fick sitt e-postkonto utsatt för intrång, men brydde sig inte eftersom det enligt hennes uppfattning inte fanns något av värde i kontot. Respondent 1 och 3 nämner att de använder enklare och samma lösenord till konton som kräver regelbunden inloggning och innehåller mindre känsliga data. De uttrycker att de föredrar en bekvämligare och mindre komplicerad hantering, även om de vet om att det kan medföra risker. Detta visar att användarupplevelsen av snabb inloggning på sina konton är viktigt för respondenterna, i synnerhet om värdet av kontot innehåller mindre känsligdata.

Vidare har tvåfaktorsautentisering varit förekommande bland respondenterna. Detta beror dels på ovannämnda temat men förknippas även till temat ”förebyggande automationsprocess”, dvs funktionen av att ett system automatiskt uppmärksammar när något misstänksamt inträffar och gör något förebyggande såsom att skicka varningsmeddelande eller automatisk vidarebefordring till skräppost för skadliga e-post. Respondenterna har berättat om varningsmeddelanden och liknande företeelser vilket passar in i detta tema. Inget har tytt på att interna säkerhetsprocesser inom system har utgjort en fara för studenterna utan snarare har det haft på positiv inverkan. Respondent 1, 3 och 7 nämner exempelvis på sådana automatiska förebyggande processer. Detta tema identifierats även inom uppfattningen kring antivirus samt lösenordsskapande genom att vissa webbsidor numera bland annat kräver starkt lösenord för att skapa ett konto och varnar om ett lösenord är svagt, likt vad respondent 4 och respondent 6 nämnde.

5.3 Användning och uppfattning av antivirusprogram

I detta stycke analyseras och diskuteras respondenternas förståelse och hantering av antivirusprogram samt faktorerna som bidrar till deras beteende.

Inom ramen av antivirus har uppfattningarna och tankarna varierats där temat kring det förebyggande automationsprocessen är aktuellt. En respondent nämnde explicit att hon tog det för givet att antivirus kommer förinstallerat vid köpet vilket är en möjlig indikation på när för mycket tillit till automatiserade processer kan ha möjlig negativ påverkan, genom att den egna vaksamheten sänks, vilket Pfleeger m.fl. (2017) menar är en del av skyddsmekanismerna. Totalt övervägt har empirin visat att automationsprocesser har haft en effektiv roll i det förebyggande arbetet. Detta må dels vara varför varierande tankar finns kring antivirus, varför

studenterna inte utsätts för ännu fler attacker genom att systemen blockar det iförhand samt varför privat data inte delats ut, genom exempelvis varningsmeddelanden vid anslutning till offentliga nätverk eller i samband med betalning via mobil bank ID.

Det ekonomiska temat har diffusa knytningar till antivirus. Endast en respondent av alla hade betalt antivirusprogram installerat, vilket är en möjligtvis kan förklara att studenter inte vill betala för antivirus även om cybersäkerhetsmedvetenheten generellt såg bra ut. Majoriteten av respondenterna hade antingen antivirus nedladdat genom gratis nedladdning eller genom att det var förinstallerat, vilket även knyter det till temat om förebyggande automationsprocesser. Av relevans blir då hur en analys kring hur attityden påverkar studenternas uppfattning och implementering av antivirus. Olika attityder identifierades rörande antivirus vilket kan sammanfattas till passivitet, negativitet och positivitet. De mer passiva tendenserna reflekterar majoriteten av studenterna som hade antivirus men gratis versioner förutom respondent 5 som kände till fördelarna av antivirus men ändå inte hade något installerat alls. Detta återspeglas av respondent 5, 6 och 7. Respondent 6 sade att hon känner stark tillit till hennes operativsystem och inte ägnar tankar åt antivirusprogram medan respondent 7 var osäker på att hon hade antivirus utan tog för givet att det kommer förinstallerat. Dessa attityder tyder på ett passivt ställningstagande och agerande gentemot antivirus. De mer negativa attityderna uttrycktes av respondent 4 & respondent 6 vilket uppfattades påverka prestanda och användarvänligheten. De positiva attityderna återges av respondent 2 som använder gratis antivirusprogram tillsammans med VPN och av respondent 9 som tyckte om funktionen av hennes antivirus.

6 Slutsats

Frågeställningen för studien är ”*Hur medvetna är svenska högskolestudenter om informationssäkerhet & cyberattacker och hur relaterar detta till deras faktiska beteenden?”*

Studien har kommit till underfund med att svenska högskolestudenter inom IT och datavetenskap har en adekvat nivå av cybersäkerhetsmedvetenhet. Majoriteten av studenterna förstår att cybersäkerhet handlar om att skydda privat data från obehöriga och har en bra förståelse för olika typer av cyberattacker, hot samt risker. Vissa studenter hade en lägre cybersäkerhetsmedvetenhet, det kan dels vara på grund av deras låga uppfattning om risknivå eftersom de inte känner sig som sannolika måltavlor, de antar att de tekniska skyddsåtgärderna de använder är tillräckliga vilket kan leda till minskad personlig vaksamhet och att de prioriterar bekvämlighet över säkerhetsrutiner.

Ett annat viktigt resultat som visade sig i studien är kunskapskällan som bidrog till respondenternas aktiva säkerhetsbeteenden. Flera av de respondenterna som visade på säkert beteende var till en följd av direkt eller indirekt erfarenhet av en IT-attack och på grund av informell kunskapsinhämtning. Detta visar att studenternas tendens att vidta säkerhetsåtgärder ökar när de personligen upplever konsekvenserna av en IT-attack, lär sig om attacker vid sociala sammanhang såsom närvaro inom spelvärlden eller via sociala medier och nyheter.

Att studenterna hade goda kunskaper om IT-attacker tack vare spelvärlden är ett unikt fynd i jämförelse med tidigare forskning som har nämnts i denna studie. Denna data kan användas till att ge fler möjligheter att skapa lättillgänglig information som når ut till alla i och med att det krävs olika inlärningsmetoder för att säkerställa hög medvetenhet och aktivt agerande.

7 Rekommendationer och framtida forskning

För att öka cybersäkerhetsmedvetenheten bland högskolestudenter rekommenderar författarna därför att det är viktigt att satsa på spridning av information via olika kanaler och metoder. I universiteten bör det finnas genomgående information för att agera som en påminnelse och ingå i olika sammanhang. Informell utbildning via evenemang, workshops, kampanjer, sociala medier, reklam och dylikt bör även utökas eftersom detta kan vara mer lockande för studenter att självmant gå av intresse vilket kan leda till en kedjereaktion att fler börjar bli intresserade. Dessa moment bör dock vara lockande och skulle till en början kunna ingå i andra typer av kampanjer för att uppmärksammas.
Författarna rekommenderar att det hade varit av forskningsfältets intresse att studera en större skala av studenter för att få ett mer validerat svar på forskningsfrågan, bland annat genom att undersöka studenter utanför IT och datavenskap. Detta hade även kunnat göras med hjälp av en enkätstudie för att samla in stora mängder av respons för att kunna analysera vilka faktorer som särskiljer sig mellan olika grupper baserat på datorvana, utbildningsprogram, ålder, kön, erfarenhet etc. Det hade även varit av intresse att simulera verkliga attacker för dessa respondenter för att se deras faktiska beteende från deras påstådda.

7.1 Begränsningar

Det bör noteras att denna studie inte är omfattande i dess analys av cybersäkerhet och skyddsmekanismer som tillfrågades studenterna och bör därför inte betraktas en holistisk förståelse över svenska studenters cybersäkerhetsmedvetenhet.

8 Referenslista

Abbas, H., Amjad, M.F., Atiquzzaman,M., Ashfaq, U., Bin Shahid, W., Emmanuel,N., Iqbal, Zafar., Shafqat, Narmeen., Tanveer, A., Yaqoob, T. (2023). Security Assessment and Evaluation of VPNs: A Comprehensive Survey. [Elektroniskt]. *Amc computing Surveys*, Vol. 55 (13), ss. 1-47. Tillgänglig: Business Source Ultimate [2024-04-24]. DOI: 10.1145/3579162.

Albayrak, E., Bagci, H. (2022). Modelling the effects of personal factors on information security awareness [Elektronisk]. *Journal of information Science*, ss 1. Tillgänglig: Business Source Ultimate [2024-04-28]. DOI: 10.1177/01655515221127609.

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. I *Proceedings of the 2018 IEEE TALE Conference*. ss.

1-6. 4-7 December, 2018, Wollongong, Australien. Tillgänglig: IEEE [2024-02-27] DOI: 10.1109/TALE.2018.8615162

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. [Elektronisk]. *Big Data Cogn. Comput*, Vol. 5(2), Tillgänglig: Business Source Ultimate [2024-03-10]. DOI: 10.3390/bdcc5020023.

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, Vol. 12(5), ss. 2589. Tillgänglig: Scopus [2024-02-23] DOI:10.3390/app12052589

An, Q., Cheong Hin Hong, W., Xu, X., Zhang, Y., & Kolletar-Zhu, K. (2022). How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates. [Elektronisk]. *International Journal of information Security*, Vol. 22 (2), ss. 305 - 317. Tillgänglig: Business Source Ultimate [2024-03-24]. DOI: 10.1007/s10207-022-00637-z.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. [Elektronisk]. *Computers in Human Behavior*, Vol 29(3), ss. 706-714. Tillgänglig: Science Direct [2024-03-20] DOI: 10.1016/j.chb.2012.12.018

Backman, J. (2016) Rapporter och uppsatser. 3. Uppl. Lund: Studentlitteratur

BBC (2007). *Bank loses $1.1m to online fraud*. London: BBC. Tillgänglig: http://news.bbc.co.uk/2/hi/business/6279561.stm [2024-03-06]

Bounfour, A., Dieye, R., Ozaygen, A., Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks [Elektronisk]. *Risk management & Insurance Review*, Vol. 23(2), ss 183- 208. Tillgänglig: Business Source Ultimate [2024-04-28]. DOI: 10.1111/rmir.12151

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology [Elektronisk]. *Qualitative Research in Psychology*, vol. 3(2), ss. 77–101. Tillgänglig: Taylor & Francis. [2024-05-27] DOI: 10.1191/1478088706qp063oa.

Denscombe, M. (2017) *The Good Research Guide – for small-scale social research projects*. Översatt av P. Larsson. Lund: Studentlitteratur.

ENISA (2023a) *Threat Landscape 2023* (Rapport) [Elektronisk] Athen: ENISA. Tillgänglig: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 [2024-02-27]

ENISA (2023b) *Identifying emerging cyber security threats and challenges for 2030* (Rapport) [Elektronisk] Athen: ENISA. Tillgänglig: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030 [2024-02-27]

Erbschloe, M (2019) *Social Engineering : Hacking Systems, Nations, and Societies*. Uppl 1. Förlagsort: Boca Raton: CRC Press. Tillgänglig: EBSCO DOI: 10.1201/9780429322143 [2024-03-07]

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity Awareness in Online Education: A Case Study Analysis. [Elektronisk] *IEEE Access*, vol. 10, ss. 52319-52335. Tillgänglig: IEEE [2024-03-01] DOI: 10.1109/ACCESS.2022.3171829.

International Telecommunications Union (ITU), *Definition of cybersecurity*. Genéve: ITU. Tillgänglig: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [2024-02-29]

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. [Elektronisk] *Computers in Human Behavior*, Vol 66, ss 75-87.Tillgänglig: Scopus [2024-03-20] DOI: 10.1016/j.chb.2016.09.012

Kungliga Tekniska Högskolan (2024). *Inaguration of Sweden's first cybercampus*. Stockholm: KTH. Tillgänglig: https://www.kth.se/en/om/nyheter/centrala-nyheter/sveriges-nya-cybercampus-invigt-1.1314934 [2024-03-10]

Moallem, A. (2019) Cyber Security Awareness Among College Students. [Elektronisk] I *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity.* 21-25 Juli, 2018, Orlando, Florida. Tillgänglig: Scopus [2024-02-27] DOI: 10.1007/978-3-319-94782-2_8

Oliveira, L., Chmielewski, A., Rutecka, P., Cicha, K., Rizun, M., Torres, N., & Pinto, P. (2023). Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus - A Case Study of Higher Education Institutions in Portugal and Poland. *I 2023 IEEE International Conference on Cyber Security and Resilience*. 31 juli -2 augusti, 2023, Venedig, Italien, Tillgänglig: IEEE [2024-02-26] DOI: 10.1109/CSR57506.2023.10224910

Pfleeger, C., P, Pfleeger, S. L. & Margulies, J. (2015). *Security in computing*. 5. uppl. [Elektronisk] London: Pearson. Tillgänglig: Amazon [2023-01-15].

Regeringskansliet (2023). *Regeringen satsar på svenskt cybercampus vid KTH*. Stockholm: Utbildningsdepartementet. Tillgänglig: https://www.regeringen.se/pressmeddelanden/2023/09/regeringen-satsar-pa-svenskt-cybercampus-vid-kth/ [2024-03-26]

Revilla, L., Montoya, J., & Ramamoorthi, L. (2023). Exploring Cybersecurity Awareness Among Students from Two Latin American Universities: An Empirical Analysis. [Elektronisk]. *2023 World Engineering Education Forum-Global Engineering Deans Council (WEEF-GEDC)*, Vol. 10(2), ss.1-7. Tillgänglig: EBSCOhost [2024-02-27] DOI: 10.1080/19393555.2022.2088428

Slusky, L. och Partow-Navid, P. (2012) Students Information Security Practices and Awareness [Elektronisk] *Journal of Information Privacy and Security*, Vol. 8(4), ss. 3–26. doi: 10.1080/15536548.2012.10845664. Tillgänglig: Taylor & Francis [2024-02-26]

Shukla, S. S., Tiwari, M., Lokhande, A. C., Tiwari, T., Singh, R., & Beri, A. (2022). A Comparative Study of Cyber Security Awareness, Competence and Behavior. I *5th International Conference on Contemporary Computing and Informatics (IC3I)*. 14-16 December, 2022, Uttar Pradesh, Indien. Tillgänglig: IEEE. [2024-02-22] DOI: 10.1109/IC3I56241.2022.10072880

Verizon (2023) *2023 Data Breach Investigations Report* (Rapport) [Elektronisk] Tillgänglig: https://www.verizon.com/business/resources/T2b4/reports/2023-data-breach-investigations-report-dbir.pdf [2024-02-07]

Vetenskapsrådet (2017). *God forskningssed*. Stockholm: Vetenskapsrådet.

Yin, L., Fang, B., Guo, Y., & Sun, Z. (2020). Hierarchically defining Internet of Things security: From CIA to CACA [Elektronisk]. *International Journal of Distributed Sensor Networks*, Vol. 16(1), Tillgänglig: Directory of Open Access Journals [2024-03-20] DOI: 1550147719899374.

9 Bilagor

9.1 Bilaga 1 Intervjumall

Introduktion

- "Tack för att du tar dig tid att delta i denna intervju. Syftet med vår studie är att förstå hur svenska högskolestudenter uppfattar informationssäkerhet och IT-attacker. Dina svar är värdefulla och kommer att behandlas konfidentiellt. Är det okej att vi spelar in detta samtal för forskningsändamål?"

Bakgrundsinformation

1. "Kan du börja med att berätta lite om dig själv, din studieinriktning och din årskurs?"
2. "Hur skulle du beskriva din dagliga användning av internet och digitala enheter?"

Uppfattningar och Erfarenheter

3. "Vad kommer först till ditt sinne när du hör termerna 'informationssäkerhet' och IT säkerhet?? Kan du ge exempel?"
4. "Har du eller någon du känner någonsin varit utsatt för en IT-attack? Kan du berätta om situationen och hur den påverkade din uppfattning av IT säkerhet?"

Kunskap och Attityder

5. "Hur bedömer du din egen kunskapsnivå när det gäller informationssäkerhet och skydd mot IT-attacker? Finns det olika IT attacker du känner till"
6. "På vilket sätt har du skaffat dig kunskap om informationssäkerhet? Är det genom utbildning, personliga erfarenheter, eller på annat sätt?"

Beteenden och Strategier

7. "Vilka specifika åtgärder tar du för att skydda dig själv online? Kan du nämna några exempel på säkerhetsaspekter du använder?"
8. "Hur påverkar din uppfattning om IT-säkerhetsrisker ditt beteende på internet? Ändrar du ditt beteende beroende på vilken typ av aktivitet du utför online?"
9. Finns det någon gång då din uppfattning om risk med IT-säkerhet skiljt sig från dina faktiska beteenden online? Kan du ge ett exempel?

Förebyggande och Utbildning

9. "Vilken typ av information eller utbildning anser du vore mest effektiv för att öka medvetenheten om informationssäkerhet bland studenter?"
10. "Finns det något mer universiteten eller andra organisationer kunde göra för att förbättra säkerhetsmedvetenheten och skyddet mot IT-attacker bland studenter?"

11. "Ser du någon skillnad i medvetenhet och beteenden kring informationssäkerhet mellan dig och dina kamrater? Finns det gemensamma missförstånd eller kunskapsluckor som du har märkt?"

Avslutande

11. "Finns det något annat du skulle vilja tillägga som vi inte har täckt i denna intervju, som du anser är viktigt för vår förståelse av informationssäkerhetsmedvetenhet bland högskolestudenter?"

Avslutning

- "Tack så mycket för din tid och dina insikter. Din input är mycket värdefull för vår forskning. Om du har några frågor om studien eller önskar mer information, tveka inte att kontakta oss. Tack igen."

9.2 Bilaga 2 Reviderad intervjumall

Introduktion

Tack för att du tar dig tid att delta i denna intervju. Syftet med vår studie är att förstå hur svenska högskolestudenter uppfattar cybersäkerhet och IT-attacker. Dina svar är värdefulla och kommer att behandlas konfidentiell. Intervjun kommer att anonymiseras.
Är det okej att vi spelar in detta samtal för forskningsändamål?

Bakgrundsinformation

Kan du börja med att berätta lite om dig själv, din studieinriktning och vilket år du läser?

Hur skulle du beskriva din dagliga användning av internet och digitala enheter?

Uppfattning

Vad Känner du till om IT-säkerhet eller cybersäkerhet? – kan du ge exempel
- Finns det olika IT-attacker du känner till?

Kunskap och attityder + erfarenheter

Hur bedömer du din egen kunskapsnivå när det gäller informationssäkerhet och skydd mot IT-attacker

På vilket sätt har du skaffat dig kunskap om informationssäkerhet?
- Är det genom utbildning, personliga erfarenheter, eller på annat sätt
Har du eller någon du känner någonsin varit utsatt för en IT-attack? Kan du berätta om situationen och hur den påverkade din uppfattning av IT säkerhet?

Beteenden och strategier

Allmänt

Vilka specifika skyddsåtgärder tar du för att skydda dig själv online?
Kan du nämna några exempel?

Lösenordshantering

Beskriv din process för att skapa och hantera lösenord
Har du samma lösenord till alla plattformar
Vart sparar du dina lösenord
Hur ofta ändrar du lösenord
Delar du med dig av det till andra

Uppdatering och antivirus

Beskriv hur du gör när du laddar ner ett program.
Har du antivirusprogram nedladdat?
- Vet du vad den har för syfte?
Hur ofta uppdaterar du programvaror?

Phishing

Har du delat din personliga information online (känslig info.), och i så fall, hur tänker du kring det?

Har du någonsin blivit kontaktad av någon som du **inte** känner via e-post, sociala medier eller telefon, och som bad dig om personlig information eller att utföra en handling? -Hur hanterade du situationen?

Vilka tecken tror du tyder på att en person eller webbplats kan försöka manipulera dig online?

-Vad känner du till med riskerna med att klicka på okända länkar eller öppna bilagor från okända avsändare?

Allmänt

Finns det någon gång då din uppfattning om it-säkerhetsrisker skiljt sig från dina faktiska beteenden online? Kan du ge ett exempel?

Förebyggande och utbildning

Skulle du vilja utveckla din cybersäkerhetsmedvetenheten?
Om ja - Vilket sätt hade varit mest gynnsamt för dig?

Vilka åtgärder tycker du bör tas för att öka medvetenhet om IT-attacker?

Finns det något mer universiteten eller andra organisationer kunde göra för att förbättra cybersäkerhetsmedvetenheten bland studenter?

HÖGSKOLAN VÄST
Institutionen för ekonomi och IT
Avdelningen för informatik
461 86 TROLLHÄTTAN
Tel 0520-22 30 00
www.hv.se