LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Allmänhetens medvetenhet av ID-kapningar vid olika social engineering attacker

En enkätstudie utförd på privatpersoner

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Anna Knutsson
Daniel O'Brien

Handledare: Benjamin Weaver

Rättande lärare: Björn Svensson
Markus Lahtinen

Allmänhetens medvetenhet av ID-kapningar vid olika social engineering attacker: En enkätstudie utförd på privatpersoner

ENGELSK TITEL: Public awareness of the risks of identity theft during different social engineering attacks: A survey performed on private individuals

FÖRFATTARE: Anna Knutsson och Daniel O'Brien

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, PhD

FRAMLAGD: augusti, 2022

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 60

NYCKELORD: Social Engineering, Informationssäkerhet, Medvetenhet, Allmänheten

SAMMANFATTNING (Max. 200 ord):

I vårt samhälle används idag tekniker för att kunna göra flera vardagliga funktioner. Det finns dock risker med detta då det kan ge tillgång till mycket känslig information. ID-kapning är en risk som innebär att din identitet används av obehöriga på ett olagligt sätt och detta kan ske via social engineering attacker.

Syftet med arbetet är att undersöka svenska internetanvändarna medvetenhet till ID-kapning vid olika social engineering attacker. Det är även att klarlägga hur social engineering attacker används för att komma åt känslig data.

I litteraturen ges det djupare förklaring till ID-kapning, olika social engineering attacker och medvetenhet samt utbildnings påverkan på säkerhet. Vi har gjort en enkätundersökning för att få svar från allmänheten om olika attacker och säkerhetsbeteenden. Resultatet diskuteras sedan i koppling till litteraturen för att undersöka IT-säkerheten hos individer. Slutligen ser vi att phishing attack har en högre medvetenhet än waterholing, och lägst medvetenhet har attacken reverse social engineering. De med högre utbildning har högre medvetenhet och så även de som arbetar med IT.

Innehåll

Figurer

Tabeller

1 Inledning

1.1 Bakgrund

IT-säkerhet blir allt viktigare i samhället i takt med att vårt levnadssätt idag på många sätt är kopplat till olika tekniker (Hamoud & Aïmeur, 2020). Vi använder oss av internet och olika tekniker i vår vardag och är beroende av flera av det tekniker som finns, för att på ett effektivt sätt vara en del av samhället (Hamoud & Aïmeur, 2020). IT har gett oss stora möjligheter och bekvämligheter men enligt Muhirwe och White (2016) finns det risker och utmaningar, som vi kan utsättas för vid användande av dessa tekniker. ID-kapning är en risk som innebär att ens digitala identitet tas och blir tillgänglig för någon annan att använda (Polisen, 2021). Social engineering eller på svenska social manipulation är en typ av tillvägagångssätt som används för att ta del av information hos privatpersoner och utsätter dem för en risk för ID-kapning (Mouton, Leenen & Venter, 2016). Social engineering attacker innebär kort att manipulera individer genom sociala interaktioner, till att uppge känslig information som var efterfrågat av utövaren av attacken (Mouton, Leenen & Venter, 2016). Internets framväxt och dess användning gör att mycket personlig identifierbar information nu blir tillgänglig (Salam, Dai & Wang 2021). Denna information kan användas för att ta en persons online identitet men även för att kunna rikta attacker mot privatpersoner och därmed lyckas med en social engineering attack (Koyun & Al Janabi, 2017).

ID-kapning har blivit ett faktum för många svenskar och under en tidsperiod på ett år (maj 2020 - maj 2021) var det ca 192 000 personer i Sverige som blev utsatta för en ID-kapning (Mysafety, 2021). Det är även många svenskar som utsätts för försök till ID-kapning, ca 24% vilket motsvarar nästan 2 miljoner människor (Mysafety, 2021). Det finns en oro bland svenska internetanvändare för nätbedrägeri och att obehöriga ska komma åt känsliga uppgifter (Internetstiftelsen, 2021). Hamoud och Aïmeur (2020) påpekar även att attacker mot människor och deras data ökar och blir allt vanligare. De menar även på att veta hur en kan skydda sina privata uppgifter är en absolut nödvändighet och borde vara en del av utbildningen. Hamoud och Aïmeur (2020) jämför detta med att vet hur man använder internet är lika viktigt som bilkörning eller andra uppenbara färdigheter.

1.2 Problemformulering

Risken för att drabbas för en social engineering attack och därmed riskera att råka ut för en ID-kapning ökar i takt med den tiden man spenderar online (Muhirwe & White, 2016). Med tanke på att flera vardagliga funktioner kräver tid online gör det att denna risk ökar. Identitetsstöld har enligt Salam, Dai och Wang (2021) blivit ett kritiskt problem för samhället.

Det finns en rad olika konsekvenser med att någon annan har kontroll över din identitet online och vid en ID-kapning riskeras kontrollen över dessa att försvinna (Irvin-Erickson & Ricks, 2019). Exempelvis kan någon komma åt dina bankuppgifter, vilket gör att någon annan har kontrollen över dina pengar och hur det används, någon annan utger sig för att vara dig, köper varor i ditt namn, beställer kreditkort med mera (Polisen, 2021).

Wang och Liou (2021) ser att allmänheten har en grundläggande säkerhet men att användare av internet inte vet hur de ska agera för att skydda sig för säkerhetsrisker online. Det finns

flera säkerhetsåtgärder att vidta för att skydda känslig information men människan är den svagaste länk för sin säkerhet online, vilket gör att en kan utsättas för social engineering attacker (Jain, Tailang, Goswami, Dutta, Sankhla, & Kumar (2016). Genom att göra privatpersoner mer medvetna kring social engineering attacker kan det enligt Kumar, Chaudhary och Kumar (2015) minska riskerna för privatpersoner att bli offer för sådana attacker. Medvetenhet och utbildning om informationssäkerhet tar även Jaeger (2018) och Grassegger och Nedbal (2021) upp som en avgörande faktor för att öka beteenden som leder till en säkrare användning av internet och för att skydda sig mot social engineering attacker. Vi vill undersöka denna fråga och se hur medvetenheten hos privatpersoner ser ut vid olika social engineering attacker och hur det kan leda till en ID-kapning.

1.3 Syfte

Syftet med arbetet är att undersöka svenska internetanvändarnas medvetenhet av ID-kapning vid olika social engineering attacker. Det är även att klarlägga hur social engineering attacker används för att komma åt känslig data samt konsekvenserna med en ID-kapning.

1.4 Forskningsfråga

Hur medvetna anser sig svenska internetanvändare vara om social engineering attacker och hur det kan leda till en ID-kapning?

1.5 Avgränsningar

Vi har valt att kolla på social engineering attacker som sker online och mot privatpersoner och inte organisationer.

2 Litteraturgenomgång

Under kapitlet litteraturgenomgång kommer relevant fakta och teorier tas upp och förklaras. Litteraturgenomgången är uppdelad i tre delar, den första som fokuserar på ID-kapning, den andra presenterar social engineering och i tredje delkapitlet, utbildning och medvetenhet kopplat till säkerhet.

2.1 ID-kapning

2.1.1 Definition av ID-kapning

ID-kapning, även kallat identitetsstöld eller identitetsbedrägeri innebär enligt Polisen (2021) att en individs personuppgifter används för att utföra olika typer av handlingar i dennes namn. Dessa handlingar anses då vara olagliga för att någon annan har tagit denne individs identitet. På liknande sätt definierar Reyns (2013) ID-kapning som ett samlingsord som innebär olovlig användning av en individs privata information. Användningen ska enligt Reyns (2013) vara för kriminella ändamål och ske utan individens samtycke. Detta är den definitionen vi kommer utgå från genom arbetet.

Några av de brotten som identitetsstöld ofta innefattar är kreditkortsbedrägeri och andra bedrägeri, exempelvis bankuppgifter (Reyns, 2013). Polisen (2021) tar upp andra exempel på olovlig användning, exempelvis att beställa varor, köpa på kredit, få ut bankuppgifter och ta lån, allt genom dennes personuppgifter. De beskriver även att det räknas som en ID-kapning om en person kommer åt en individs sociala medier och utger sig för att vara den (Polisen, 2021). Genom att komma åt konton på internet, exempelvis sociala medier och en individs kontakter, kan det finnas risk för konversationer och att bedragaren ber kontakter om pengar eller andra uppgifter (Polisen, 2021). Irvin-Erickson och Ricks (2019) nämner också att information kring kreditkort och bankuppgifter ofta är information som tas. De beskriver ID-kapning som personlig information används utan tillåtelse av någon annan. Information om personnummer och lösenord är enligt Irvin-Erickson och Ricks (2019) också information som inte får användas utan tillåtelse, utan räknas då som en ID-kapning. Oftast utförs bedrägerierna för en ekonomisk vinning (Irvin-Erickson & Ricks, 2019).

2.1.2 Konsekvenser av ID-kapning

Konsekvenserna av en ID-kapning kan ge direkta och indirekta ekonomiska effekter, psykiska och fysiska samt sociala konsekvenser (Irvin-Erickson & Ricks, 2019). Dessa konsekvenser betonar Golladay och Holtfreter (2016) och de adderar även juridiska problem som en konsekvens. De tar även upp den tiden som kan krävas för att lösa problem som uppkommer vid en identitetsstöld, dessa kan enligt Golladay och Holtfreter (2016) ta mellan 15 - 30 timmar.

Direkta ekonomiska konsekvenser handlar om att du blir av med pengar från bankkonton (Irvin-Erickson & Ricks, 2019). Indirekta ekonomiska konsekvenser kan exempelvis vara juridiska avgifter, skadad kredit på grund av ID-kapning, skulder eller andra kostnader som behöver betalas som en följd av bedrägeriet (Irvin-Erickson & Ricks, 2019).

Andra konsekvenser som Irvin-Erickson och Ricks (2019) och Golladay och Holtfreter (2016) redogör för är psykiska och det kan innefatta skam, rädsla, ilska, misstro, minskad tillit och ångest. Fysiska konsekvenser är följder av det psykiska som kan innefatta sömnsvårigheter som leder till trötthet, sämre aptit och orolig mage (Irvin-Erickson & Ricks, 2019; Randa & Reyns, 2020). Enligt Golladay och Holtfreter (2016) kände ca 21% av dem drabbade någon typ av fysisk konsekvens och ca 80% upplevde psykiska konsekvenser. Känslomässiga konsekvenser är vanligare reaktioner på offer än fysiska effekter (Randa & Reyns, 2020).

Social påverkan kan innebära att vänner och familj riskerar att bli påverkade genom det följder ett identitetsbedrägeri kan få (Irvin-Erickson och Ricks, 2019). Ett exempel är vid en ekonomisk förlust, kan det utgöra en påverkan på den sociala miljön för den utsatta. Ekonomiska konsekvenser på grund av identitetsstöld online påverkar direkt en persons socioekonomiska status, som sen i sig kan ge psykiska konsekvenser (Hille, Walsh och Cleveland, 2015). Konsekvenserna varierar från inga till större och allvarligare hos personer som varit med om en ID-kapning (Irvin-Erickson och Ricks, 2019). Randa och Reyns (2020) ser att utbildning, nettoförlust och tiden för att lösa problemen kopplade till identietsstölden var faktorer som ökade sannolikheten för att rapportera någon typ av konsekvens.

Fear of identity theft (FOIT) delar Hille, Walsh och Cleveland (2015) upp i två dimensioner, dels rädsla för ekonomiska förluster men även rädsla för skada på ryktet. Ekonomiska förluster är som beskrivit tidigare av Irvin-Erickson & Ricks (2019). Hille, Walsh och Cleveland (2015) definer rädsla för skada på ryktet som en rädsla för att ens personuppgifter används på ett olagligt sätt i syfte som kan skada offrets rykte. Det kan skada ens namn, sociala status, påverka karriärmöjligheter med mera. Hille, Walsh och Cleveland (2015) kommer fram till att ett förbättrat förtroende online kan minska FOIT båda dimensioner, likaså kan en förbättrad integirtetsoro online komma att förbättra rädslan kring identitetsstöld.

2.1.3 Onlineaktivitet kopplat till ID-kapning

Syftet med Reyns (2013) rapport är bland annat att se över relationer var en individ och dess rutinmässiga aktiviteter online kopplat till utsatthet för ID-kapning. Åldern var en avgörande faktor, äldre personer hade en ökad risk för ID-kapning (Reyns, 2013; Mesch och Dodel, 2018). De individerna med högre inkomst va ca 60% mer benägna att utsättas för ID-kapning jämfört med de med lägre (Reyns, 2013). Andra onlineaktiviteter som enligt Reyns (2013) var riskabla var användandet av internet för bankverksamhet eller andra ekonomiska funktioner, de var ca 50% mer benägna att bli offer. Detta påstår även Mesch och Dodel (2018) som säger att finansiella aktiviteter ökar risken för att bli offer för onlinebedrägeri.

De som använde sig av e-handel hade ca 30% större risk för ID-kapning (Reyns, 2013). E-post och andra typer av meddelandetjänster online ökade risken med ca 50% (Reyns, 2013). Mesch och Dodel (2018) säger att alla kommunikationsaktiviteter online ger en ökad risk för att blir utsatt för e-post scams, vilket kan leda till en id-kapning.

Det undersöks dock inte vidare om till exempel individer med högre inkomster kanske använder sig av e-handel oftare och på så sätt ökar risken då det finns fler tillfällen att råka ut för en ID-kapning (Reyns, 2013). Reyns (2013) menar dock att även om dessa aktiviteter online ger en ökad risk så går det inte att begränsa sig från detta och ändra sitt beteende genom att sluta använda dessa onlinerutiner. Istället vill Reyns (2013) få fram att resultaten visar betydelsen

av nätverkssäkerhet och en utbildad användning av internet. Detta nämns även av Jaeger (2018) som visar vikten av att medvetenhet kring säkerhet och användning, kan ge en ökad säkerhet och på så sätt kan riskerna för användandet av onlineaktiviteter minska.

2.2 Social engineering

Social engineering kan förklaras som attacker på människor istället för system (Conteh & Schmick, 2016). Denna form av attack använder sig av människors självförtroende i sin egen förmåga att se igenom möjliga försök av bedrägeri samt deras tillit för personer i positioner av auktoritet för att komma åt system och information (Thornburgh, 2004; Conteh & Schmick, 2016). Thornburgh (2004) beskriver att de som utför social engineering attacker per definition är inte hackers själva utan hacker-enablers, i och med att informationen om användaren behöver sedan användas efter att en social engineering attack sker. Thornburgh (2004) säger dock att i många fall så är den som utför social engineering attacken, det vill säga agerar som en hacker-enabler också är hackaren. Eftersom alla system och verksamheter har en mänsklig faktor så innebär detta att det alltid kan finnas en risk för attackerna, oavsett det tekniska arbetet som ett system genomgår (Krombholz m. fl., 2015).

Social engineering attacker utvecklas ständigt i takt med att säkerhetsåtgärder och annan teknologi som blir säkrare. Krombholz m. fl. (2015) beskriver i deras artikel att det finns fyra former av attacker, varav en attack kan ingå i en eller flera av dessa grupperingar. Attackerna är följande:

- Fysiska attacker
- Sociala attacker
- Tekniska attacker
- Socio-tekniska attacker, som kan förklaras som en kombination av de två sistnämnda kategorierna.

Ivaturi och Janczewski (2011) vill istället påstå att det finns två huvudsakliga grupperingar, person-till-person och person-till-person via media. Atkins och Huang (2013) gör en mycket liknande kategorisering till den som Ivaturi och Janczewski (2011) gör, men döper istället kategorierna till human-interaction för person-till-person och computer-based interaction för person-till-person via media.

Fysiska attacker (Krombholz m. fl., 2015) är attacker som fokuserar på att hitta fysiska föremål som kan hjälpa att komma åt systemet. Krombholz m. fl. (2015) tar upp "dumpster diving" det vill säga att man gräver igenom skräp från någon för att hitta känslig data, som ett exempel. Ivaturi och Janczewski (2011) beskriver hur fysiska attacker hamnar under person-till-person, då dessa attacker kräver en närvarande person som utför attacken för att det ska kunna genomföras. Atkins och Huang (2013) kategoriserar fysiska attacker under human-interaction.

Sociala attacker är attacker som istället försöker övertyga personen att ge över data (Krombholz m. fl., 2015). Detta kan ske genom flera olika sätt, men ett vanligt sätt är att använda sig av auktoritet över användaren för att försöka komma åt datan (Krombholz m. fl., 2015). Tekniska attacker använder sig av verktyg för att söka igenom internet för data på en person i ett försök att hitta känslig information (Krombholz m. fl., 2015).

Socio-tekniska attacker är attacker som kombinerar flera olika av det tidigare nämnda formerna av attacker. Krombholz m. fl. (2015) förklarar att denna gruppering innehåller några av det starkaste formerna av social engineering attacker. Phishing är attacker som försöker få användaren att manuellt ge över känslig information, till exempel genom att uppge sig själv som banken eller microsoft genom att användaren trycker på en komprimerad länk (Conteh & Schmick, 2016). Spear-phishing attacker är istället en av det tekniska phishing attackerna med profiler byggda med hjälp av sociala attacker för att skicka phishing attacker med mycket högre träffsäkerhet, och är ett exempel på en mer effektiv socioteknisk attack jämfört med den rent tekniska attacken (Krombholz m. fl., 2015).

De två kategoriseringar som Ivaturi och Janczewski (2011) samt Atkins och Huang (2013) skapar kan täcka attacker inom tekniska, sociala såväl som sociotekniska attacktyper som Krombholz m. fl. (2015) beskriver ovan. Detta eftersom person-till-person och person-till-person via media kan använda sig av både tekniska verktyg och sociala förutsättningar, eller en kombination av båda dessa.

2.2.1 Plattformar för attacker

Krombholz m. fl. (2015) utforskar några av det tillvägagångssätt som attackeraren kan använda sig av vid försök till ID-kapning. De listar tre huvudsakliga plattformar, sociala nätverk, molntjänster och mobila applikationer. Sociala nätverk är ofta använda för en attack på grund av att det finns en enorm mängd information om användaren som har öppen åtkomst, samt hur enkelt det är för attackeraren att nå ut till personen som attacken riktades mot (Ivaturi & Janczewski, 2011). Ivaturi och Janczewski (2011) beskriver att det gör det lättare för mer personliga attacker såsom spear phishing. Utföraren av dessa mer personliga typer av attack kan bygga profiler som låtsas vara någon annan, dessa profiler kan efterlikna det riktiga profilerna till hög grad eftersom användare frivilligt delar med sig av personlig information (Krombholz m. fl., 2015).

Krombholz m. fl. (2015) beskriver riskerna med molntjänster främst ur perspektivet av ett företag, i och med att det inte finns samma kontroll över filerna jämfört med när filerna sparas lokalt och att det finns mindre tillit mellan användare och uppladdare. Detta kan dock också utnyttjas av attackeraren när det kommer till privatanvändare, i och med att privatanvändare också använder sig alltmer av fildelningstjänster. Heartfield och Loukas (2015) beskriver hur adoption av cloud och internet i alla aspekter av vardagen gör att det finns större risk för bedrägeri, som till exempel en falsk alert på ens bil som skulle kunna likna de falska virus alerter som kan ses på internet idag.

Mobila applikationer är också ett farligt tillvägagångssätt för attacker (Krombholz m. fl., 2015). Falska applikationer kan även vara en risk för mobilanvändare, applikationer som ser lika ut till den som användaren försöker hitta (Heartfield och Loukas, 2015). Dessa applikationer kan vid nedladdning till exempel fråga användaren om lov att komma åt vissa delar av mobilens känsliga data (oftast i form av en pop-up alert som användaren då kan trycka ja på utan att tänka efter) beskriver Krombholz m. fl. (2015) och Heartfield & Loukas (2015).

2.2.2 Taxonomi av Social engineering attacker

Det finns flera olika typer av attacker, och olika grupperingar sker av dessa attacker beroende på vad som spelar störst roll inom den typen av attack (Ivaturi & Janczewski, 2011; Krombholz m.fl., 2015). Exempel på några attacker är phishing, waterholing och reverse social engineering (Krombholz m. fl., 2015; Conteh & Schmick, 2016; Ivaturi & Janczewski, 2011). Phishing är attacker som försöker få användaren att manuellt ge över känslig information, till exempel genom att uppge sig själv som banken eller microsoft genom att användaren trycker på en komprimerad länk (Conteh & Schmick, 2016). Spear-phishing attacker är attacker som använder sig av profiler byggda på information från målet av attacken för att med högre träffsäkerhet övertyga dem att råka ut för attacken (Krombholz m. fl., 2015). Ivaturi och Janczewski (2011) beskriver att phishing kategoriseras som en person-till-person via media attack.

Waterholing, en teknisk eller socio-teknisk attack enligt Krombholz m. fl. (2015), är en attack där attackeraren skapar en hemsida, för att sedan attackera användaren genom hemsidan, inte helt annorlunda från phishing attacker. Det kan exempelvis vara att hemsidan är en kopia av en riktig hemsida, för att lura användare. Reverse social engineering är en attack som istället försöker få personen att vända sig till attackeraren för hjälp (Gragg, 2002; Conteh & Schmick, 2016; Krombholz m. fl., 2015). Krombholz m. fl. (2015) och Gragg (2002) beskriver detta i tre simpla steg, attackeraren skapar ett problem för personen, erbjuder sedan sin hjälp med att lösa problemet, och i processen så kommer de åt känsliga system. Gragg (2002) beskriver att denna attack gör att användaren bygger tillit i den som hjälper med det tekniska problemet, det vill säga att det byggs en relation, det andra steget i bild 1. Denna attack kategoriserar som social eller socio-teknisk (Krombholz m. fl., 2015). Conteh & Schmick (2016) beskriver en liknande attack men döper den istället "Quid pro Quo" (latin för "något för något"), som de beskriver som att en användare med tekniska problem blir lurade på deras information när de söker hjälp med problemen.

2.2.3 Faser av social engineering

Det finns flera olika sätt att genomföra en social engineer attack på men det finns några gemensamma faktorer hos alla (Salahdine & Kaabouch, 2019; Koyun & Al Janabi (2017). Det grundläggande metoden bakom dessa attacker består av fyra olika steg (Salahdine & Kaabouch, 2019). Det första handlar om att samla information om det tänkta målet. Det andra beskrivs som att skapa en typ av relation till denne. Kommande steg innebär att dra nytta av informationen som samlats och genomföra attacken för att sedan i det fjärde och sista steget avsluta utan att lämna några spår (Salahdine & Kaabouch, 2019; Koyun & Al Janabi, 2017; Conteh & Schmick, 2016).

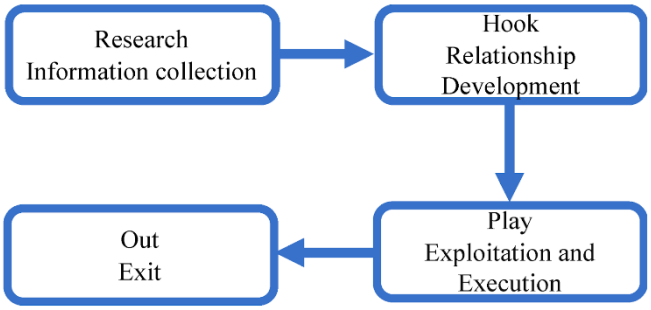


Bild 2.1: Överblick över social engineering attacker (Salahdine & Kaabouch, 2019)

Heartfield & Loukas (2015) bryter ned social engineering i tre faser: Orchestration, Exploitation och Execution. Inom dessa så finns flertal kategorier. Orchestration innefattar det förberedande stegen av en attack, Exploitation består av två kategorier som beskriver hur informationen hos offret kommer att kommas åt och Execution består av hur attacken kommer att genomföras och avslutas (Heartfield & Loukas, 2015). Denna taxonomi av en attack är en fördjupning av den social engineering hook, där Orchestration motsvarar det första och andra steget, Exploitation är del av det tredje steget och Execution är delvis det tredje steget och delvis det fjärde steget (Heartfield & Loukas, 2015; Salahdine & Kaabouch, 2019).

Orchestration, är det första steget i processen (Salahdine & Kaabouch, 2019; Koyun & Al Janabi, 2017; Conteh & Schmick, 2016; Heartfield & Loukas, 2015). Heartfield och Loukas (2015) beskriver att den första processen inom detta steg är target description, en process som definierar ett offer till attackeraren. Heartfield & Loukas (2015) beskriver vidare några steg för att fortsätta med orchestration, såsom method distribution och method of automation, den förstnämnda är då hur attacken ska nå fram och den senare nämnda till hur mycket attackeraren själv behöver utföra under attackens gång.

Det nästa steget i social engineering hook är exploitation, eller play-steget (Salahdine & Kaabouch, 2019; Koyun & Al Janabi, 2017; Conteh & Schmick, 2016; Heartfield & Loukas, 2015). Heartfield & Loukas (2015) beskriver att detta steg innehar deception vector och interfacemanipulation. Deception vector beskriver Heartfield & Loukas (2015) som i vilken utformning attacken har, och de gör två huvudsakliga grupperingar: visuella och betendee, eller en kombination av båda. Conteh & Schmick (2016) ger direkta exempel på attacker som kan kategoriseras under dessa två, visuella såsom phishing attacker med liknande länkar till hemsidan som egentligen sökes och beteende såsom reverse social engineering (Krombholz m. fl., 2015, Conteh & Schmick, 2016). Interface manipulation är på vilket sätt attacken presenteras till offret (Heartfield & Loukas, 2015).

Det sista steget i hook är execution, vilket faller under både play och out-steget (Salahdine & Kaabouch, 2019; Koyun & Al Janabi, 2017; Conteh & Schmick, 2016; Heartfield & Loukas, 2015). Execution är när attacken sker, och är då attacken avslutas (Salahdine & Kaabouch, 2019; Heartfield & Loukas, 2015). Heartfield & Loukas (2015) har två kategorier under detta steg, och används för att kategorisera attackerna efter hur många gånger användaren behöver bli lurad för att attacken ska få effekt och om attacken sker en gång eller är upprepningsbar.

2.2.4 Indikationer på social engineering attacker

Det finns flera faktorer att vara uppmärksam på för att upptäcka en eventuell social engineering attack (Koyun & Al Janabi, 2017; Greitzer, Strozer, Cohen, Moore, Mundie & Cowley, 2014). Det är viktigt att använda sunt förnuft och vara uppmärksam om något ser konstigt eller annorlunda ut berättar Koyun och Al Janabi (2017). Några av dessa kan vara dålig grammatik eller stavning, konstig eller ovanlig avsändare, annorlunda sammanhang och även felaktig information (Gretizer m. fl., 2014). Skulle det vara så att det anses vara misstankar om en social engineer attack så är det bättre att inte agera (Koyun & Al Janabi, 2017). Andra indikationer på att det är en attack på gång är faktorer som att det är brådska att fatta ett beslut eller agera (Koyun & Al Janabi, 2017; Greitzer m. fl. 2014). Det är bra att vara uppmärksam på om informationen som efterfrågas redan borde vara tillgänglig för personen/organisationen alternativt att det är information som de inte ska ha tillgång till (Koyun & Al Janabi, 2017). Det sista Koyun & Al Janabi (2017) beskriver som en faktor att uppmärksamma är om något är för bra för att vara sant, exempelvis ett mail med en vinst på en stor summa pengar eller liknande. Enligt Greitzer m. fl. (2014) så är det vanligt vis goda eller dåliga nyheter. Greitzer m. fl. (2014) tar även upp några exempel på vad som ofta är den önskade handlingen vid ett försök till social engineering attack. Specifik information eller att man ska uppdatera personlig information, en länk eller bilaga som ska klickas på eller öppnas (Greitzer m. fl. 2014).

2.3 Utbildning och medvetenhet

Hamoud och Aïmeur (2020) uppmärksammar tre faktorer som ska ledar till ett säkert beteende online och dessa är en process som inklurerar säkerhetsmedvetenhet, utbildning och träning. Vikten av medvetenhet hos internetanvändare är en faktor för att öka agerande som skyddar mot social engineer attacker (Jaeger 2018; Grassegger & Nedbal 2021; Kumar, Chaudhary & Kumar, 2015). Jaeger (2018) resonerar kring *information security awareness* (ISA), på svenska informationsäkerhetsmedvetenhet, vilken är delaktig för påverkan av ett säkrare onlinebeteende hos en individ. *Information security awareness* (ISA) innebär enligt Jaeger (2018) att ta hänsyn till en individs kunskap och förståelse kring området informationssäkerhet. Även Grassegger och Nedbal (2021) kollar vidare på teorin kring ISA.

Det går att diskutera utifrån olika nivåer men två av de som nämns av Jaeger (2018) är den individuella nivån och en social-miljö nivån, vilket sker när en individ interagerar med sin sociala miljö. Under den individuella nivån visar Jaeger (2018) att den allmänna vetenskapen kring informationssystem, har visat en ökad information security awareness (ISA), det vill säga en ökad medvetenhet kring ens säkerhet. Det är även uppvisat att en individ som blivit utsatt för en informationssäkerhetsincident tenderar att öka nivåerna kring dennes ISA (Jaeger, 2018). Detta ser även Jaeger och Eckhardt (2021) som kollar på ISA när det kommer till phishing attacker. Grassegger och Nedbal (2021) kollar på förtroende och risker som individuella faktorer som påverkar ISA. De kommer fram till att förtroende har en negativ påverkan på ISA medans riskuppfattning har en positiv koppling. En faktor som däremot minskar ISA enligt Jaeger (2018) är datorångest, vilket innebär en rädsla kring att arbeta på datorer. Under den social-miljö nivån är det genom att media och liknande lyfter säkerhetsfrågor och problem kring säkerhet som leder till en ökad ISA på grund av att det väcker intresse samt informerar kring det (Jaeger, 2018).

Information security awareness (ISA) påverkar attityder och beteende direkt och indirekt enligt Jaeger (2018). Det visade bland annat att en ökad informationssäkerhetsmedvetenhet, leder till en ökad attityd om att använda teknologier för säkerhet som till exempel anti-spyware program, samt ökade även användningen av brandvägg (Jaeger, 2018). ISA har en god effekt för handlingssätt som stödjer säkerheten för privatpersoner (Jaeger, 2018). På liknande sätt visar Grassegger och Nedbal (2021) att ISA har en effekt för agerandet för att skydda sig mot social engineering attacker. De påstår dock att det endast har indirekta effekter och inte direkta som Jaeger (2018) säger. Enligt Grassegger och Nedbal (2021) så påverkar medvetenheten attityden och det i sig leder till avsikten att motstå social engineering attacker. Jaeger och Eckhardt (2021) ser att vid phishing attacker kopplat till ISA, är det att användarna ser attacken som ett hot och blir då rädda och att det sedan är rädslan som i sin tur framkallar en motivation till att vidta skyddsåtgärder. Det är på så sätt faktiska agerande som stärker deras säkerhet sker när det gäller phishing attacker (Jaeger & Eckhardt, 2021). Även i detta fallet blir det som en indirekt påverkan på agerandet liksom Grassegger och Nedbal (2021) beskriver.

Muhirwe och White (2016) kommer även de fram till att med en högre cybersäkerhet medvetenhet påverkar en individs cybersäkerhetspraxis. Muhirwe och White (2016) definierar medvetenhet som en kombination av kunskap (vad användarna vet), attityd (vad de tänker) och beteende (vad de gör). Enligt Muhirwe och White (2016) ökar medvetenheten genom utbildningar inom cybersäkerhet. I detta fallet poängterar Muhirwe och White vikten av att göra det hos studenter då de är uppväxta med IT och använder många tjänster online samt spenderar mycket tid online, vilket ökar risken för att utsättas för social engineering attacker. De anser även att många av tjänsterna som är kopplade till skolans aktiviteter är online och därför bör det finnas utbildning om hur de säkert använder dessa tjänster (Muhirwe och White, 2016). Hamoud och Aïmeur (2020) håller med om att onlineskydd borde vara en del av utbildningen och men tycker att det ska starta i barndomen, något som skiljer sig från Muhirwe och White (2016).

Arisya, Ruldeviyani, Prakoso och Fadhilah (2020) utgår från en awareness modell gjord av Kruger och Kearney, för att kunna kategorisera de olika nivåerna av medvetenhet. De delar upp i tre olika nivåer låg, medel och bra (Arisya m. fl., 2020). Dålig / låg (poor) tillhör resultaten med en procent mindre än 59, medel (average) motsvarar 60-79% och bra / hög (good) är det mellan 80-100%.

2.4 Oro kopplat till nätbedrägeri

Användare av onlineaktiviteter kopplade till internetbank och shopping, visar en högre nivå av rädsla för att bli utsatt för identitetsstöld (Choi, Kruis, Choo, 2021). Vad rädslan enligt Choi, Kruis och Choo (2021) tros bero på är det negativa konsekvenser som en identitetsstöld kan innebära.

Nätbedrägeri är en stor orosfaktor bland användare av internet i Sverige. 9 av 10 personer känner oror för att bli utsatta för nätbedrägeri (Internetstiftelsen, 2021). För ca 4 av 10 personer är den oron stor och för ca 2 av 10 personer är oron mycket stor (Internetstiftelsen, 2021). I europa så visar en undersökning att ca 46% är oroliga över att någon ska missbruka ens

personliga data (European Commission, 2020). Denna siffra har även gått upp något under de senare åren (European Commission, 2020).

Mer specifikt svarar 66% att de är oroliga över identitetsstöld samt att andra cyberbrott som innebär förlorandet av personuppgifter ligger alla på över 50% (European Commission, 2020).

Åldersmässigt så känner yngre minst oro och de äldre känner mest oro för nätbedrägeri (Internetstiftelsen, 2021). Det är enligt Brands och van Wilsem (2021) även så att äldre känner en större oro för ekonomisk brottslighet online. Jämför man oron med antal drabbade för bedrägeri på nätet så är yngre mindre drabbade, med den lägsta oron av alla åldersgrupper (Internetstiftelsen, 2021). De äldre är även mindre drabbade av bedrägeri men med högst oro. 70- till 90-talister har störst risk för att drabbas av bedrägeri på nätet, dock visas det inte genom en stor andel "mycket stor oro" bland dessa åldersgrupper, i kontrast till utsattheten (Internetstiftelsen, 2021).

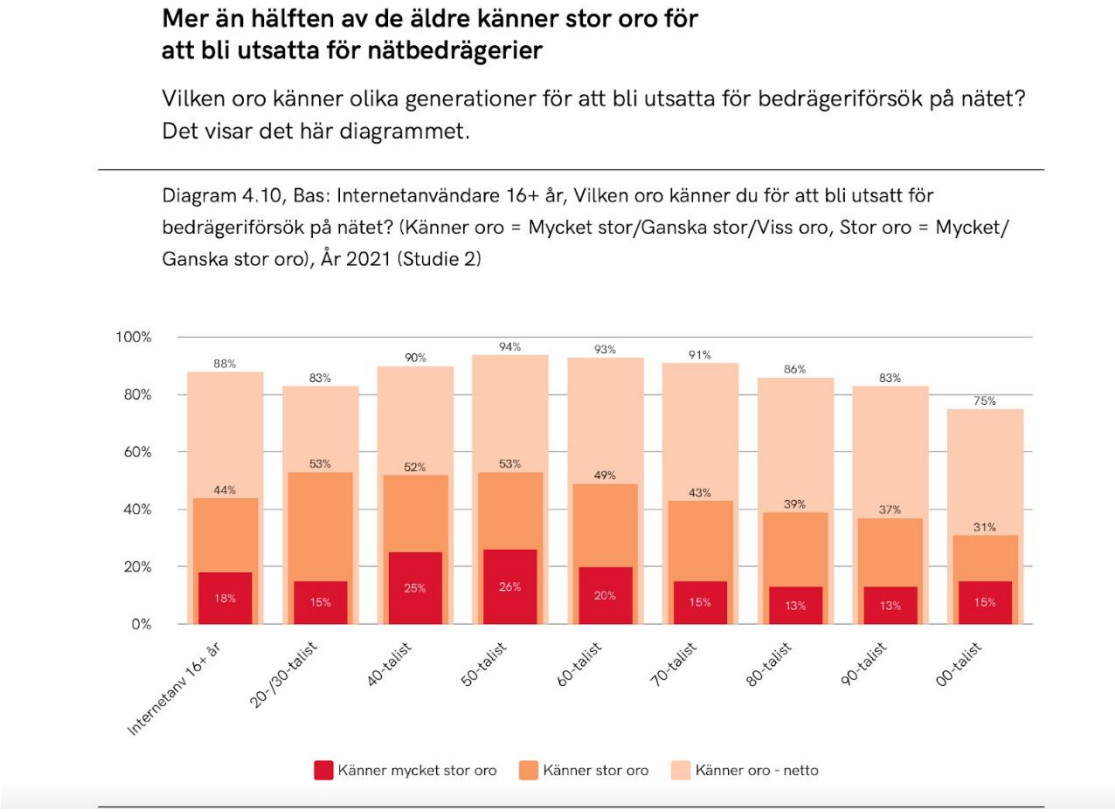


Bild 2.2: Oron kring utsatthet för nätbedrägeri (Internetstiftelsen, 2021)

Bland dem som känner stor oro och faktiskt blir drabbade, skiljer sig när utbildningsnivån analyseras (Internetstiftelsen, 2021). Av de som känner stor oro så är det 47% av de med grundskoleutbildning och 42% med högskoleutbildning. Detta stämmer överens med Brands och van Wilsem (2021) som säger att det finns en lägre nivå av rädsla bland högutbildade. Brands och van Wilsem (2021) lägger även till att de i höginkomsthushåll har en lägre rädsla. Bland dem som har blivit utsatta för identitetsstöld, har enligt Internetstiftelsen 26% haft en grundskoleutbildning och 49% högskoleutbildning. Undersökningen gäller de som blivit utsatta för antingen ett bedrägeri eller bedrägeriförsök på nätet under det senaste 12 månaderna (Internetstiftelsen, 2021). Det säger dock Mesch och Dodel (2018) emot, de påstår att

de med lägre utbildning har en större sannolikhet till att reagera på bedrägeriförsök än de med högskoleutbildning.

Anledningar till att personer undviker e-tjänster diskuteras av Internetstiftelsen (2021). Den främsta anledningen som uppges av de som avstår e-tjänster grundar sig i en oro att ens personuppgifter ska bli stulna av en hackare (Internetstiftelsen, 2021). Det är en skillnad i ålder, där det visar att äldre personerna är mer oroliga över hackare än yngre personer. Totalt sett så är det ca 14% som undviker en e-tjänst för att oron för hackare gör de så osäkra. Bland internetanvändarna födda 1920- och 30-talet är denna siffra 25% (Internetstiftelsen, 2021). Dessutom så visar Brands and van Wilsem, 2021 att 28% håller till en hög grad med om att de är oroliga för att deras bankuppgifter blir tillgängliga för obehöriga via internetbank.

Det finns en stor oro för att någon annan ska komma åt ens personuppgifter vid olika onlineaktiviteter (Internetstiftelsen, 2021). En av aktiviteter är vid betalning över nätet, delen vid betalning som skapar osäkerhet är att det ska lämna ut konto- och kortuppgifter (Internetstiftelsen, 2021). Denna rädsla är dock grundad i att informationen ska tas av någon, att någon annan kommer åt personuppgifter och risken för att bli hackad (Internetstiftelsen, 2021). Rädslan för säkerheten vid online betalning visas enligt European Commission (2020) vara på ca 41%.

Enligt European Commission (2020) så är totalt sett 52% enligt dem själva väl informerade med riskerna av cyberbrott. Uppdelat över länderna anses 72% av Sveriges befolkning vara väl informerade, vilket är den tredje högsta siffran i Europa.

Tabell 2.1: Litteratursammanställning

Område	Undersökningsområden	Litteratur
ID-kapning	Definition av ID-kapning	Polisen (2021) Reyns (2013) Irvin-Erickson och Ricks (2019)
	Konsekvenser av ID-kapning	Irvin-Erickson och Ricks (2019) Golladay och Holtfreter (2016) Randa och Reyns (2020) Hille, Walsh och Cleveland (2015)
	Onlineaktivitet kopplat till ID-kapning	Reyns (2013) Mesch och Dodel (2018) Jaeger (2018)
Social engineering	Förklaring av social engineering - Fysiska attacker - Sociala attacker - Tekniska attacker - Socio-tekniska attacker	Krombholz m. fl. (2015) Thornburgh (2004) Conteh & Schmick (2016) Ivaturi & Janczewski (2011) Atkins och Huang (2013)
	Plattformar för attacker	Krombholz m. fl. (2015) Ivaturi och Janczewski (2011) Heartfield och Loukas (2015)

	Taxonomi av en social engineering attack Social engineering faser	Krombholz m. fl. (2015) Salahdine och Kaabouch, (2019) Koyun och Al Janabi (2017) Heartfield & Loukas (2015) Gragg (2002) Conteh & Schmick (2016) Ivaturi & Janczewski (2011)
	Indikationer på social engineering attacker	Koyun och Al Janabi (2017) Gretizer m. fl. (2014)
Utbildning och medvetenhet	Utbildning och medvetenhet	Hamoud och Aïmeur (2020) Jaeger (2018) Grassegger och Nedbal (2021) Kumar, Chaudhary & Kumar (2015) Jaeger och Eckhardt (2021) Muhirwe och White (2016) Arisya m. fl. (2020)
Inställning till nätbedrägeri	Oro kopplat till nätbedrägeri	Internetstiftelsen (2021) Choi, Kruis, Choo (2021) European Commission (2020) Brands och van Wilsem (2021) Mesch och Dodel (2018)

3 Metod

Under detta kapitel presenteras först den valda litteraturundersökning. Sedan beskrivs metoden, urvalet och utformning av enkät. Följt av en diskussion kring studiens kvalitet i form av validitet, reliabilitet och etik. Kapitlet avslutas med en kort förklaring till hur resultatet presenteras.

3.1 Litteraturundersökning

Litteraturen som används är en blandning mellan akademiska källor och icke-akademiska källor. Akademiska källor har använts vid genomgång av det olika typerna av social engineering attacker. Det sektioner som berör olika typer av social engineering attacker i enkäten är attacker som var mest relevanta för det vi undersöker. Akademiska källor har också använts för att ge bakgrund som leder fram till problemområdet och sedan fortsatt för att argumentera och resonera kring ämnet social engineering för att kunna besvara frågeställningen. För att förstå begreppet ID-kapning och ge läsaren fakta kring detta så användes både akademiska och icke-akademiska källor för att få en djuphet och flera perspektiv. Personers beteende om säkerhet online diskuteras också och där används akademiska och icke-akademiska källor.

Icke-akademiska källor användes framförallt för att ge en bakgrund och för att binda det akademiska underlaget med verkligheten. Dessa källor används även för att definiera begrepp och ge större förståelse till problematiseringen. Det användes även för en del statistik för att ge förståelse till hur utbrett ämnet är.

Vi använde oss av Google Scholar, och AIS eLibrary för att hitta vetenskapliga artiklar. Vi använde oss sedan av LUBsearch vilket är Lunds universitetbibliotekstjänst, för att få åtkomst till vissa artiklar. Vi gjorde avgränsningar i sökandet i form av årtal för att informationen skulle vara inom en tidsram som fortfarande kan anses vara relevant. Vi har även kollat på antalet citeringar och läst sammanfattningar för att välja ut vilka artiklar vi ska använda. Sökorden som användes för att hitta artiklarna var "social engineering", "identity theft", "information security", "Information Security Awareness", "ID fraud", "risks", "consequences", "knowledge". Oftast används en kombination eller variationer på dessa sökord. Vi använde även Google Search för icke-akademiska källor såsom MySafety och Polisen. Sökord som användes var "ID-kapning" och "identitetsstöld".

3.2 Enkät

3.2.1 Motivering av vald metod

Valet av metod grundar sig i att kunna besvara frågeställningen. Eftersom vi vill nå ut till allmänheten så har vi valt att utföra en enkätundersökning. Enkäten riktar sig till svenska internetanvändare vilket gör att vi kan få in många svar. Syftet med enkäten är att få svar på hur allmänhetens ser på sin medvetenhet vid social engineering attacker och hur det kan leda till en ID-kapning. Samt i en kombination med frågor kring utbildning, arbete och bekvämlighet kunna dra slutsatser och diskutera medvetenhet och beteende i samhället från slutanvändarnas

håll. Vi vill göra en kvantitativ analys, detta eftersom en enkätstudie är användbar för att studera trender och mönster i en större befolkning genom ett mindre urval (Oates, 2006).

3.2.2 Urval

Enkäten var publicerad och möjlig att svara på i en vecka, mellan den 21/4 till 28/4. Enkäten delades på Facebook och fick 110 svar. Ingen inloggning eller annan identifikation behövdes för att svara på enkäten. Enkäten söker att få svar från allmänheten med inga särskilda förkunskaper inom området, därför finns det inte några andra krav för att svara på enkäten.

Vi är medvetna om att urvalet inte blir helt representativt då vi når ut till personer i vår närhet och inte allmänheten i stort. Vi tror dock att det blir tillräckligt för att kunna dra en slutsats kring hur allmänhetens medveten ser ut angående social engineering attacker och ID-kapning.

3.2.3 Utformning av enkät

Enkäten är uppdelad i tre delar, varav två som används i denna rapport. Den första består av frågor om personernas bakgrund och demografi. Den andra delen utvärderar respondentens förståelse kring flera olika attacker. Den tredje delen undersöker respondenternas inställning till BankID, men används inte i och med att syftet och forskningsfrågan på rapporten har fokuserats på social engineering attacker.

Enkäten presenteras till respondenterna genom att kort förklara vad syftet med den är, vilka det är som utför den, vilket arbete den kommer användas i och en mailadress för kontakt ifall det finns frågor eller önskemål från de som svarade på enkäten. Majoriteten av frågorna är med svarsalternativ som respondenten får klicka i med tre stycken frågor som är öppna för respondenten att skriva i själva. Frågorna med svarsalternativ är gjorda som obligatoriska för att inte respondenten ska missa någon.

Den första delen är demografiska frågor för att möjliggöra djupare analys av svaren.

Den andra delen kan brytas ned till de olika attackerna som vi frågar om, och syftet med dessa frågor är att besvara vilka sorters attacker som användare känner till. Detta för att ge förslag på vad för svagheter som förekommer i allmänhetens uppfattning av attacker på internet.

De tre attacker som har valts är tre attacker som beskrivs av Krombholz m. fl. (2015) i deras rapport, samt Ivaturi och Janczewski (2011), Conteh och Schmick (2016) och Gragg (2002). Enkäten frågar om just dessa attacker eftersom dessa attacker anses vara mycket utbredda former av social engineering attacker. Enkäten har avgränsats här genom att inte i detalj fråga om varenda sort av attack som en person kan råka ut för, detta för att hålla enkäten tillräckligt kort för att få in svar. Enkäten avgrenas in i olika följdfrågor beroende på vad personen svarar, för att endast ge respondenten relevanta frågor beroende på tidigare svar. Detta minskar också risken för förvirring hos respondenten, vilket ger bättre resultat att analysera. Eftersom enkäten riktar sig brett och inte skickas ut till större delar av befolkningen så har vi försökt göra den så lätt som möjligt att svara på, för att vi ska kunna få in så många svar som möjligt. I denna del finns frågor som är öppna för att personen ska kunna förklara, om utsatt för en attack, hur denne gick till. Detta är ingen obligatorisk fråga då vi inte vill tvinga respondenten att förklara men ändå kunna slutföra enkäten. Den frågan anser vi inte vara den viktigaste och därför vill vi hellre se ett större antal svar, än hur specifika attacker gick till.

Svarsalternativen på fråga 9, 14 och 19 kan bli lite missvisande då det kan vara en kombination av flera, medan respondenten bara gav möjlighet att besvara en av de fem alternativen. Exempelvis så kan "Dålig grammatik" kan gå in i alternativet om att hemsidan inte såg rätt ut. Vi har valt att bara tillåta ett svarsalternativ så att respondenten behöver fundera på vilket var den största anledningen till att de undvek attacken.

3.2.4 Validitet

Frågorna i enkäten har till största del färdiga svarsalternativ, men det finns några frågor som är öppna där respondenten själv kan skriva. Dessa frågor är användbara för att fånga alla det möjliga svaren som en respondent kan ha på en särskild fråga, men kan också vara svåra att analysera och kräver mer från respondenten (Oates, 2006). Validiteten av svaren kan därför vara lägre på dessa frågor.

Oates (2006) förklarar att det finns flera olika aspekter som är viktiga vid design av en enkät för att ha en hög nivå av validitet på enkäten. De viktiga aspekterna är att frågorna inte är för långdragna, att de är relevanta till enkätens ämne, att de inte är svåra att förstå, att frågorna är fokuserade på vad de försöker fråga och att frågorna inte är ledande. Detta är något vi har försökt uppfylla i vår enkät, men är lite svårt att göra då vi försöker undersöka personens vetskap kring de attacker som finns i enkäten. Därför så är det med avsikt en del av enkäten att en som svarar på den kan sakna kunskap kring det som frågas efter. Dock erbjuder vi svarsalternativ som reflekterar personens avsaknad av kunskap kring ämnet.

Medvetenhet, eller på engelska awareness, definieras som att en person förstår att ett fenomen existerar och händer (Merriam-webster, n.d.). I kontext av denna uppsats så använder vi medvetenhet i forskningsfrågan för att undersöka en privatpersons förståelse av vilka attacker som finns och om de har råkat ut för dem, för att sedan möjliggöra identifikation av vilka grupper av människor som har störst risk för att råka ut för dessa attacker. Våran enkät ämnar att besvara denna forskningsfråga genom att direkt fråga privatpersoner vilka attacker de kan identifiera efter en kort förklaring av typerna av attack.

3.2.5 Reliabilitet

Oates (2006) beskriver att reliabilitet innebär att enkäten får samma svar om den är utförd på samma respondenter. Oates (2006) förklarar dock att det kan vara svårt att mäta reliabilitet, i och med att det finns en stor mänsklig faktor med att undersöka en större grupp av allmänheten. Eftersom våran enkät undersöker allmänhetens uppfattning finns det möjlighet för lägre reliabilitet då uppfattningen hos en person kan ändras mellan svarstillfällen, men detta är en naturlig följd av den typ av enkät som vi genomför. Hög validitet leder också till högre reliabilitet, då tydliga, väldefinierade frågor gör det lättare att få liknande resultat vid upprepade tillfällen.

3.2.6 Etik

Oates (2006) förklarar att det finns fem rättigheter för respondenten. Dessa är:

- Rätten att inte delta
- Rätten att avbryta undersökningen
- Rätten att ge informerat samtycke
- Rätten till anonymitet
- Rätten till sekretess.

Eftersom enkäten endast delas på sociala medier så finns det inte något tvång att svara på den. Den som svarar på enkäten kan även avbryta när som helst. I enkäten finns en introduktion högst upp som tydliggör vilka vi är och vad vi vill uppnå, som är tillgänglig innan personen börjar med frågorna. Enkäten använder sig inte heller av någon sorts av identifiering, dessutom så kommer möjliga identifierande frågor inte kopplas med de demografiska frågorna. Enkätens enstaka svar kommer inte heller delas vidare, utan endast diagram skapade med svaren. Därmed så uppfyller vi de fem rättigheterna som Oates (2006) beskriver. Dock beskrivs det även att dessa inte är hårda och fasta regler, utan att varje forskningstillfälle måste analyseras var och för sig. Vi anser att vi inte gör någon research som, förutom de fem riktlinjerna ovan, behöver någon särskild etikkomittés godkännande.

Enkäten har möjlighet för besvararen att fylla i information själva om attackerna i slutet av varje sektion ifall de har svarat att de blivit offer för en attack tidigare i samma sektion. Detta är en öppen fråga som är helt frivillig att svara på. Detta gör att vi inte kan kontrollera det som skrivs i dessa fält för att skydda besvararen eller att det hålls relevant och kopplat till ämnet i fråga. Detta är en möjlig etisk konflikt med enkäten som den är nu. För att minska möjligheten till identifierande information i analysen så kommer svaren till dessa frågor analyseras helt separat från tidigare identifierade frågor. Dock kommer frågor med betygsgrad analyseras i samband med de demografiska frågorna för att möjliggöra mer relevanta slutsatser i analysen av enkätresultatet.

3.2.7 Presentation av resultat

Resultatet presenteras med en blandning av cirkeldiagram, även så kallade tårtdiagram, och horisontella stapeldiagram. Detta eftersom cirkeldiagram är mycket användbara för att visualisera en uppdelning av svarsalternativ på ett simpelt sätt, särskilt när det är flera men under sju kategorier beskriver Oates (2006). De horisontella stapeldiagrammen används för att gruppera staplarna efter olika demografiska frågor, som sedan är uppdelade procentuellt efter svaren inom dessa grupper. Detta för att visualisera förändringar mellan bland annat åldersgrupperna.

4 Resultat

Detta kapitel består av resultatet av de svaren vi fick på enkäten. Kapitalet delas upp efter ämnena på frågorna i enkäten. Först redovisas svaren på det demografiska frågor. Följt av de tre olika attackerna waterholing, phishing och reverse social engineering. Resultatet redovisas i form av olika tabeller och med en kort beskrivande text.

4.1 Demografiska frågor

1. Hur gammal är du?

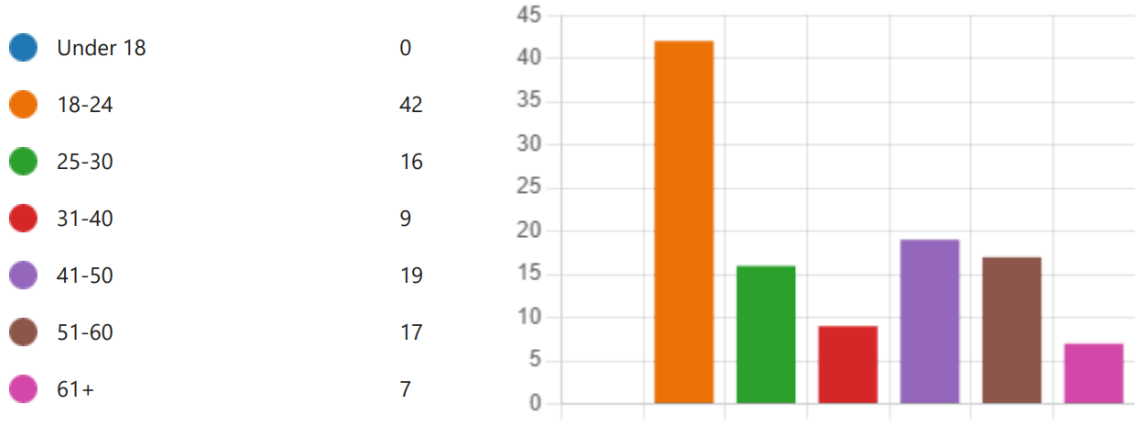


Bild 4.1: Stapeldiagram Fråga 1

Av de 110 svaren svarade 42 (38,18%) av respondenter svarade att de var mellan 18-24 år gamla, 16 (14,55%) svarade mellan 25-30 år, 9 (8,18%) svarade 31-40 år, 19 (17,27%) svarade 41-50 år, 17 (15,45%) svarade 51-60 år och 7 (6,36%) svarade att de var över 60 år.

2. Vilken är din högsta utbildningsnivå?

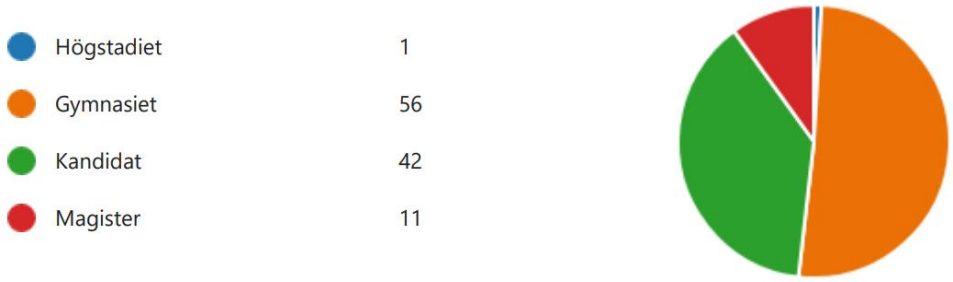


Bild 4.2: Cirkeldiagram Fråga 2

Frågan om utbildningsnivå svarade 1 (0,91%) person att de har studerat upp till en högstadienivå, 56 (50,91%) personer att de hade studerat upp till och med gymnasiet, 42 (38,18%) personer att de hade studerat på en kandidatnivå och 11 (10%) som har studerat upp till och med en magisternivå.

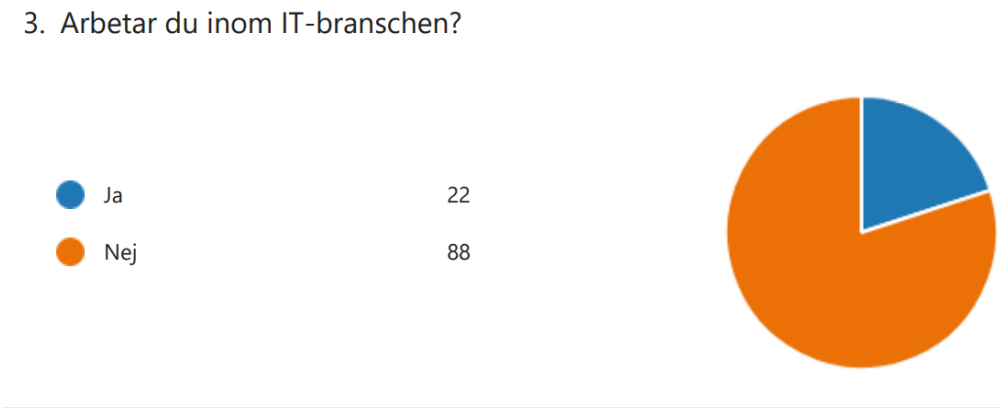


Bild 4.3: Cirkeldiagram Fråga 3

22 (20%) respondenter svarade att de arbetar inom IT-branschen, resterande 88 (80%) svarade nej på den frågan. En förklaring till att 20% svarat ja på denna är för att enkäten var delad bland våra klasskamrater som studerar IT och även jobbar inom den branschen.

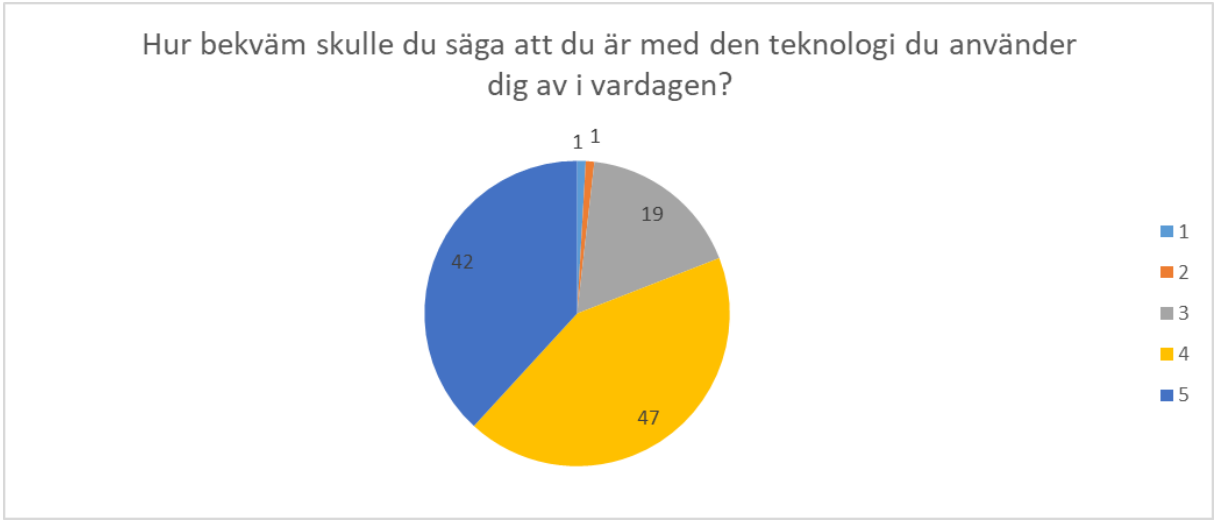


Bild 4.4: Cirkeldiagram Fråga 4

På frågan om hur bekväma de var med deras vardagliga teknologi så hamnade genomsnittet på 4,16 av 5. 1 respondent svarade 1 (0,91%), 1 (0,91%) person svarade 2, 19 (17,27%) personer svarade 3, 47 (42,73%) personer svarade 4 och 42 (38,18%) personer svarade 5. Vi kan se att totalt sätt så känner sig många respondenter bekväma med sin vardagliga teknologi.

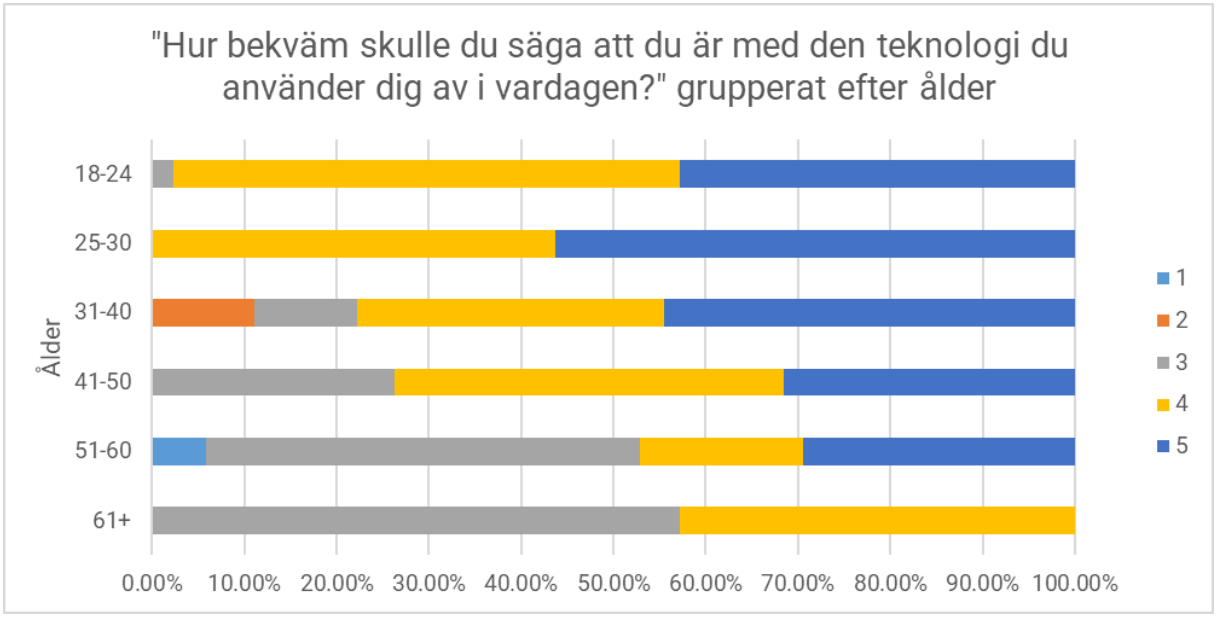


Bild 4.5: Stapeldiagram Fråga 4 grupperat efter ålder

Efter att resultaten blir uppdelade efter åldersgrupp så ser vi en trend i att de yngre svarar att de är mer bekväma med den teknologi som de använder sig av i vardagen i jämförelse med äldre.

4.2 Waterholing

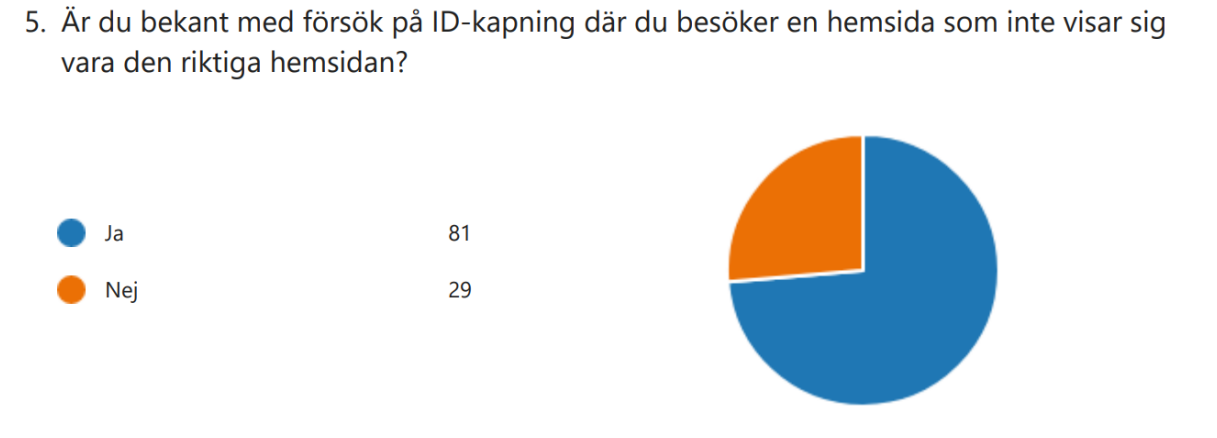


Bild 4.6: Cirkeldiagram Fråga 5

Den andra sektionen av enkäten frågar om hur bekanta respondenterna är med attacker där respondenten besöker en hemsida som inte visar sig vara den riktiga hemsidan, waterholing som diskuterat tidigare i rapporten. 81 (73,64%) personer svarade att de var bekanta med den attacken efter de läste den korta förklaringen längst upp i sektionen, medan 29 (26,36%) svarade att de inte var bekanta.

Bild 4.7: Cirkeldiagram Fråga 6

Vidare svarade 83 (75,45%) personer att de aldrig råkat ut för en sådan attack själva. 25 (22,73%) personer svarade "Ja, men jag undvek attacken", 2 (1,82%) personer svarade ja, att de råkat ut för en sådan attack.

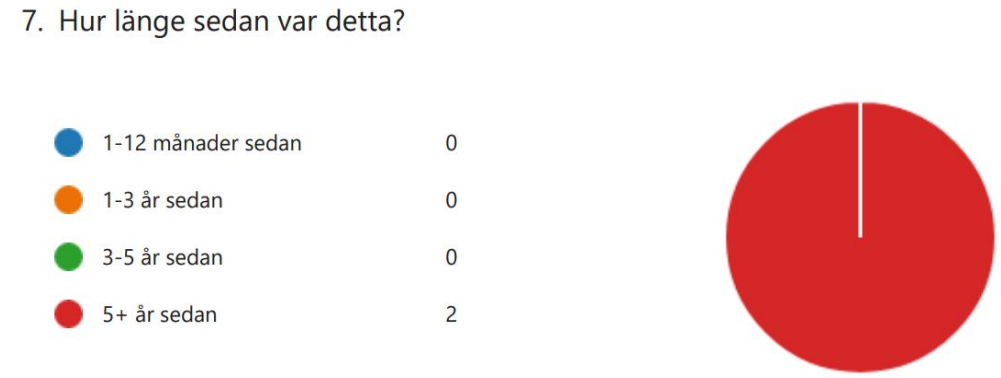


Bild 4.8: Cirkeldiagram Fråga 7

Båda som svarade "Ja" på den förra frågan blev också frågade när den attacken skedde, och båda svarade för över 5 år sedan. En av de som svarade "Ja" på frågan förklarade att deras kompis hade blivit av med sin mobil utomlands, och att bedrägeriet skedde genom en falsk länk till en Find my IPhone kopia. Personen i fråga loggade in på sidan då de "Blev stressad då jag tänkte att personen som startat telefonen kanske stänger av igen, så jag skyndande att klicka på länken. Tyckte adressen såg trovärdig ut och hemsidan såg ut precis som iCloud".

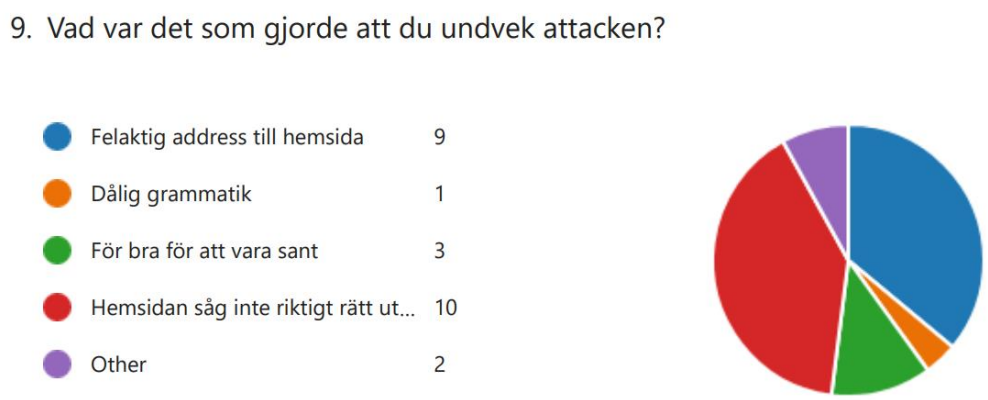


Bild 4.9: Cirkeldiagram Fråga 9

Frågan om varför de undvek attacken, så svarade 9 (36%) att de identifierade URL-adressen som felaktig, 1 (4%) person svarade att dålig grammatik på hemsidan var avslöjande, 3 (12%) svarade att det såg för bra ut för att vara sant, 10 (36%) svarade att hemsidan såg inte riktigt rätt ut i jämförelse med vad de förväntade sig, och 2 (8%) svarade övrigt.

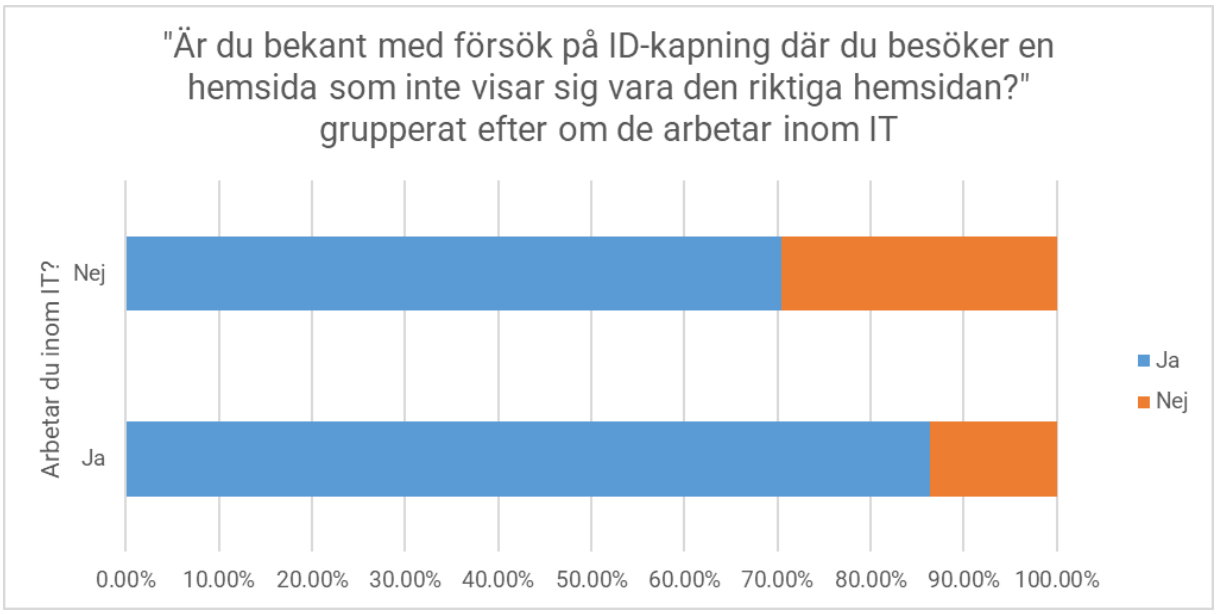


Bild 4.10: Stapeldiagram Fråga 5 grupperat efter om de arbetar inom IT

19 (86,36%) av respondenterna som arbetar inom IT kände igen denna typ av attack, 3 (13,64%) gjorde inte det. Utav de 88 som inte arbetar inom IT svarade 62 (70,45%) att de var bekanta med denna typ av attack och 26 (29,55%) personer att det inte var det.

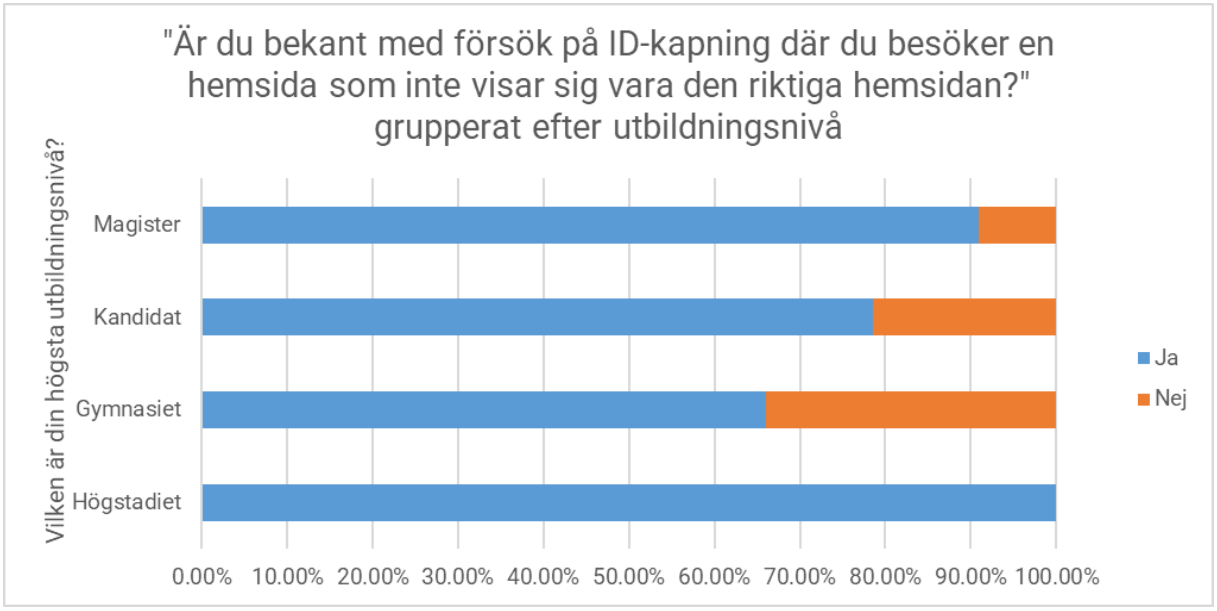


Bild 4.11: Stapeldiagram Fråga 5 grupperat efter utbildningsnivå

En person med högstadiet som utbildningsnivå svarade att de var bekant med denna typ av attack. Utav de som hade en gymnasieutbildning som högsta utbildningsnivå så var 37 (66,07%) personer bekanta med denna typ av attack och 19 (33,93%) personer var inte det. På kandidatnivå så var 33 (78,57%) personer bekanta, medan 9 (21,43%) inte var det. 10 (90,91%) personer av de med en magister som högsta utbildningsnivå svarade att de kände igen typen av attack, medan 1 (9,09%) person svarade att de inte var det.

4.3 Phishing

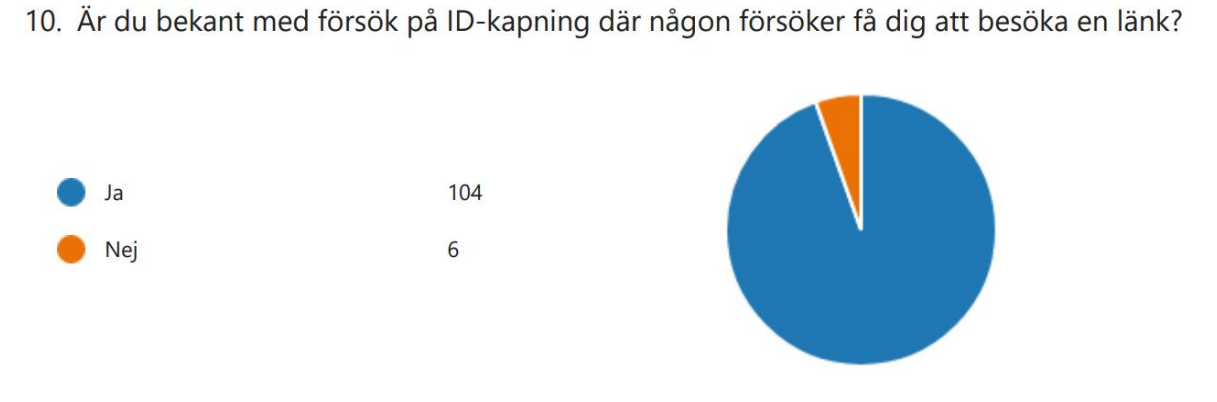


Bild 4.12: Cirkeldiagram Fråga 10

Efter en kort förklaring av attacker som försöker få personen att aktivt besöka en länk, phishing, så svarade 104 (94,55%) personer att de var bekanta med den typen av attack, och 6 (5,45%) personer svarade nej.

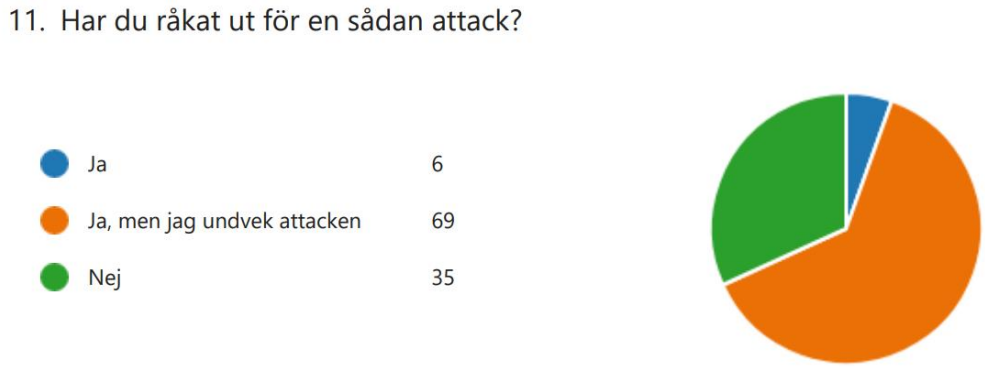


Bild 4.13: Cirkeldiagram Fråga 11

På frågan om respondenterna hade råkat ut för en sådan attack svarade 6 (5,45%) personer ja och 35 (31,82%) personer svarade nej. En majoritet svarade "Ja, men jag undvek attacken", vilket utgjorde 69 (62,73%) personer.

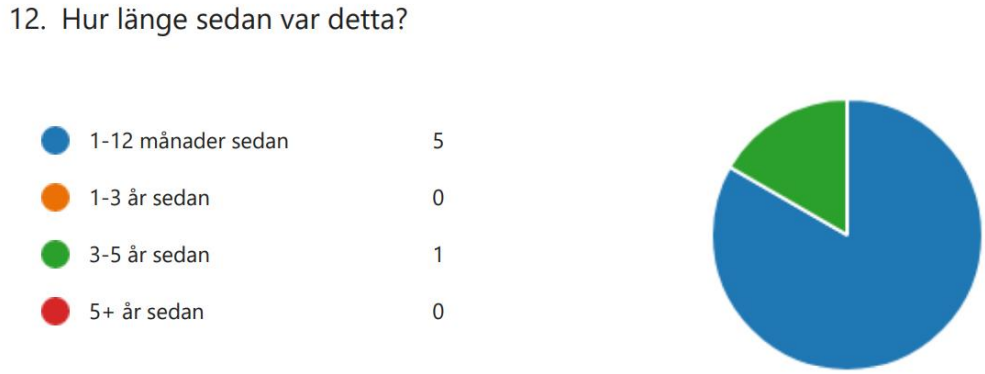


Bild 4.14: Cirkeldiagram Fråga 12

Utav de 6 som svarade ja så svarade 5 (83,32%) personer att attacken skedde nyligen, 1-12 månader sedan. Den sista respondenten (16,66%) svarade att det skedde 3-5 år sedan. Utav de som svarade "Ja" på frågan förklarade några vad som hände i det öppna svarsfältet, och deras svar beskriver hur det ofta rör sig om direkt meddelande på Facebook eller via SMS vart de får en sådan felaktig länk.

Bild 4.15: Cirkeldiagram Fråga 14

Utav de 69 personer som svarade att de hade undvikit attacken så svarade 32 (46,38%) att de tyckte att länken som de blev skickade inte såg korrekt ut. För 17 (24,64%) personer så var grammatiken avslöjande för attacken. 13 (18,84%) personer tyckte att det var för bra för att vara sant. 2 (2,9%) tryckte på länken och insåg att det inte var den länk de hade tänkt sig, medan 5 (7,25%) personer undvek attacken av övriga skäl.

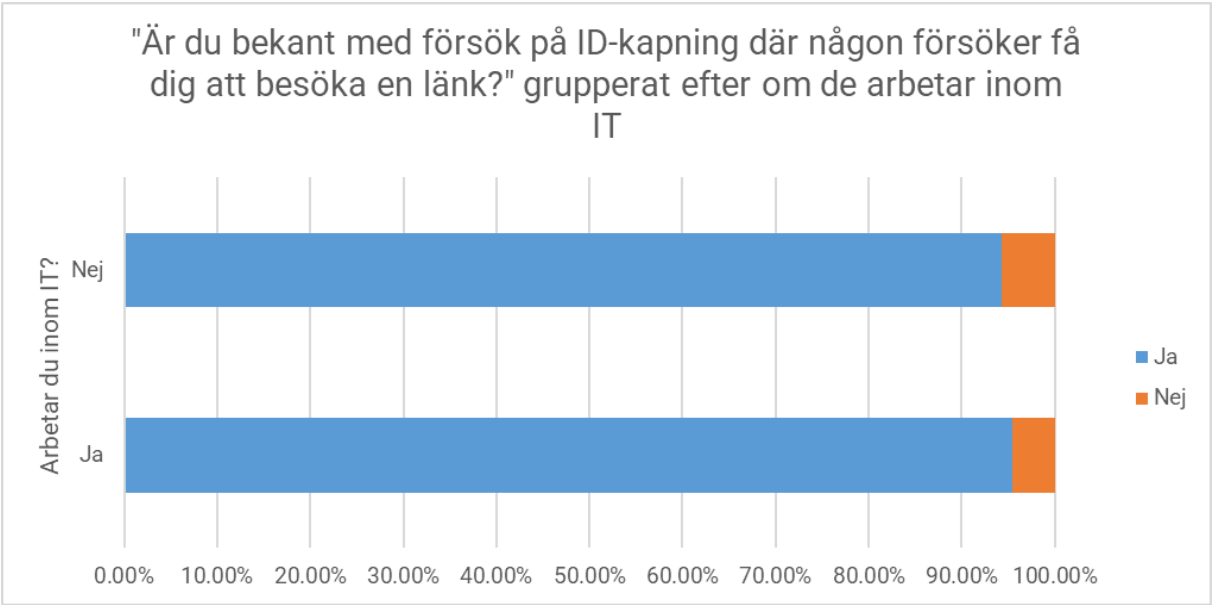


Bild 4.16: Stapeldiagram Fråga 10 grupperat efter om de arbetar inom IT

Utav de som inte arbetar inom IT så var 83 (94,32%) respondenter bekanta med denna typ av attack, och 5 (5,68%) var inte det. Av de 22 som arbetar inom IT så var 21 (95,45%) personer bekanta med denna typ av attack och en (4,55%) var inte det.

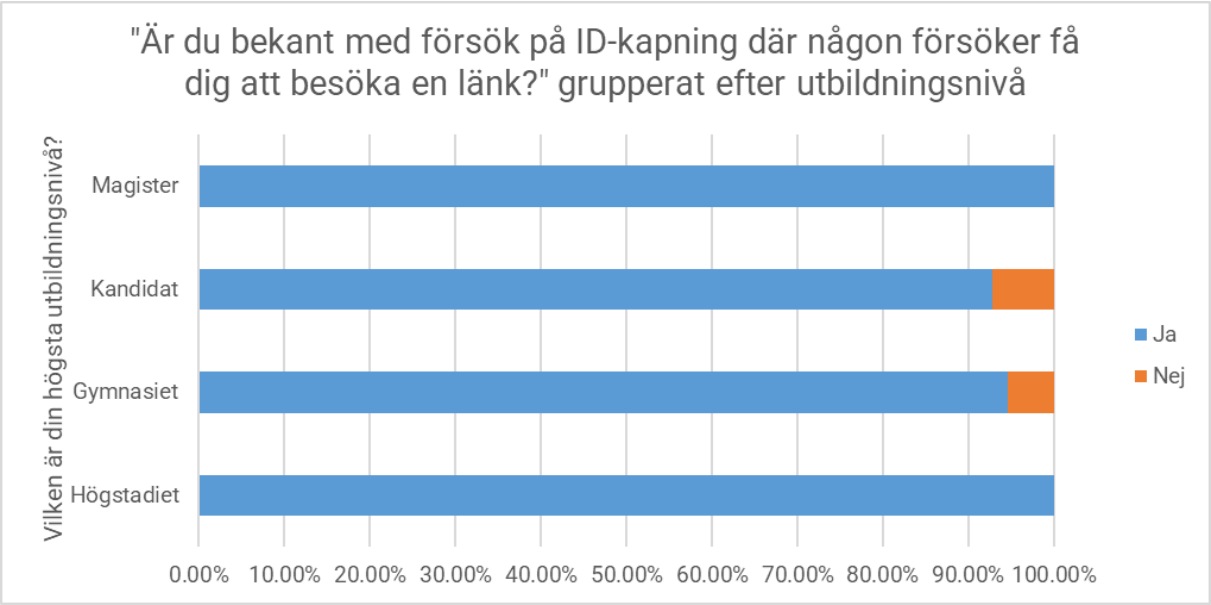


Bild 4.17: Stapeldiagram Fråga 10 grupperat efter utbildningsnivå

En person med högstadiet som utbildningsnivå svarade att de var bekanta med denna typ av attack. Utav de 56 med en gymnasieutbildning som högsta nivå så var 53 (94,64%) respondenter bekanta med denna typ av attack, och 3 (5,36%) var inte det. 39 (92,86%) personer av de med en kandidat som högsta utbildningsnivå svarade att de var bekanta med denna typ av attack och 3 (7,14%) var inte det. 11(100%) personer av de som svarade att magister var deras högsta utbildningsnivå svarade att de var bekanta med denna typ av attack.

4.4 Reverse social engineering

Bild 4.18: Cirkeldiagram Fråga 15

Efter en kort förklaring av den typen av attack som tidigare beskrivs som en reverse social engineering, så svarade 57 (51,82%) personer att de var bekanta med denna typ av attack, medan 53 (48,18%) svarade nej.

Bild 4.19: Cirkeldiagram Fråga 16

Utav dessa svarade 93 (84,55%) personer att de inte hade råkat ut för en sådan attack, 15 (13,64%) personer svarade "Ja, men jag undvek attacken", och 2 (1,82%) personer svarade att de hade råkat ut för attacken.

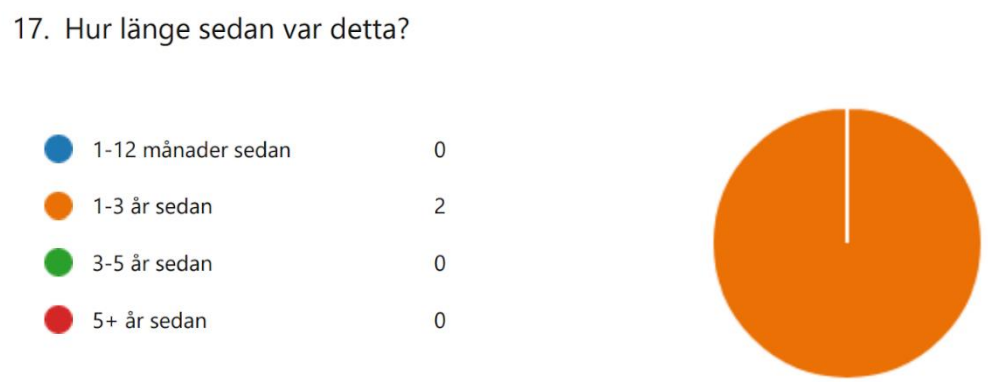


Bild 4.20: Cirkeldiagram Fråga 17

Båda de respondenter som svarade att de hade råkat ut för en sådan attack svarade att det skedde mellan 1-3 år sedan.

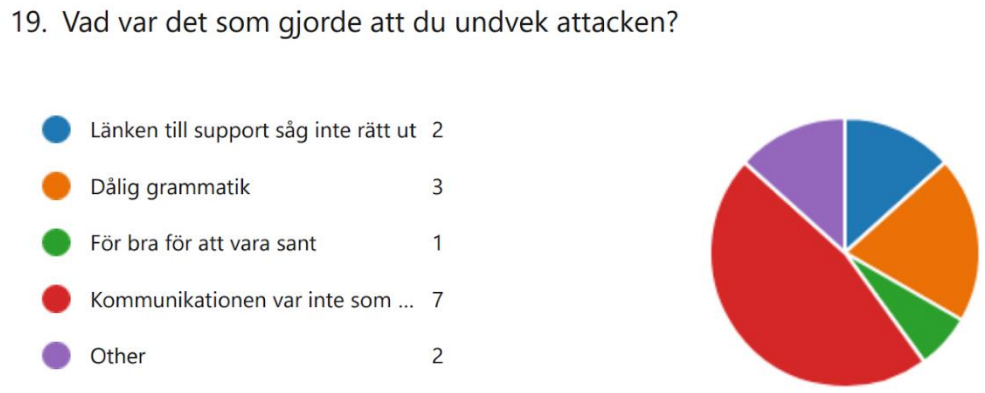


Bild 4.21: Cirkeldiagram Fråga 19

Utav de 15 som svarade "Ja, men jag undvek attacken", så svarade 2 (13,33%) personer att länken till support inte såg rätt ut. 3 (20%) respondenter svarade att dålig grammatik var avslöjande, 1 (6,67%) person svarade att erbjudandet var för bra att vara sant, 7 (46,67%) personer svarade att kommunikationen inte var som förväntad. 2 (13,33%) personer svarade att övriga skäl gjorde att de undvek attacken.

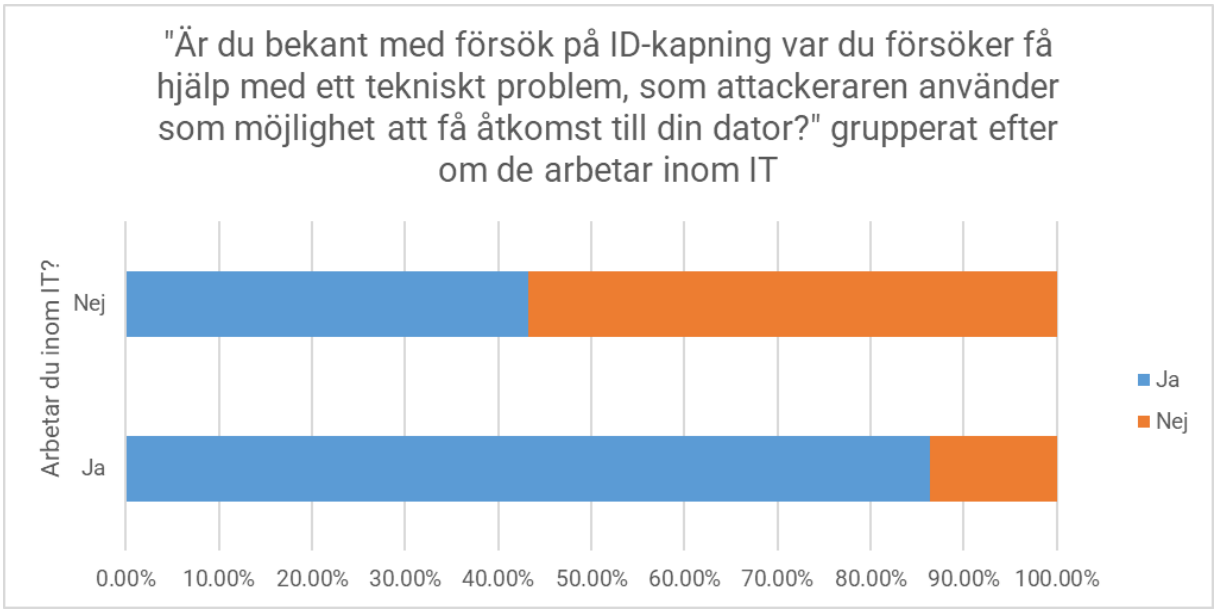


Bild 4.22: Stapeldiagram Fråga 15 grupperat efter om de arbetar inom IT

Av de som arbetar inom IT så svarade 19 (86,36%) personer att de var bekanta med denna typ av attack och 3 (13,64%) svarade att inte var det. 38 (43,18%) personer av de som inte arbetar inom IT svarade att de kände igen attacken och 50 (56,82%) svarade att de inte gjorde det.

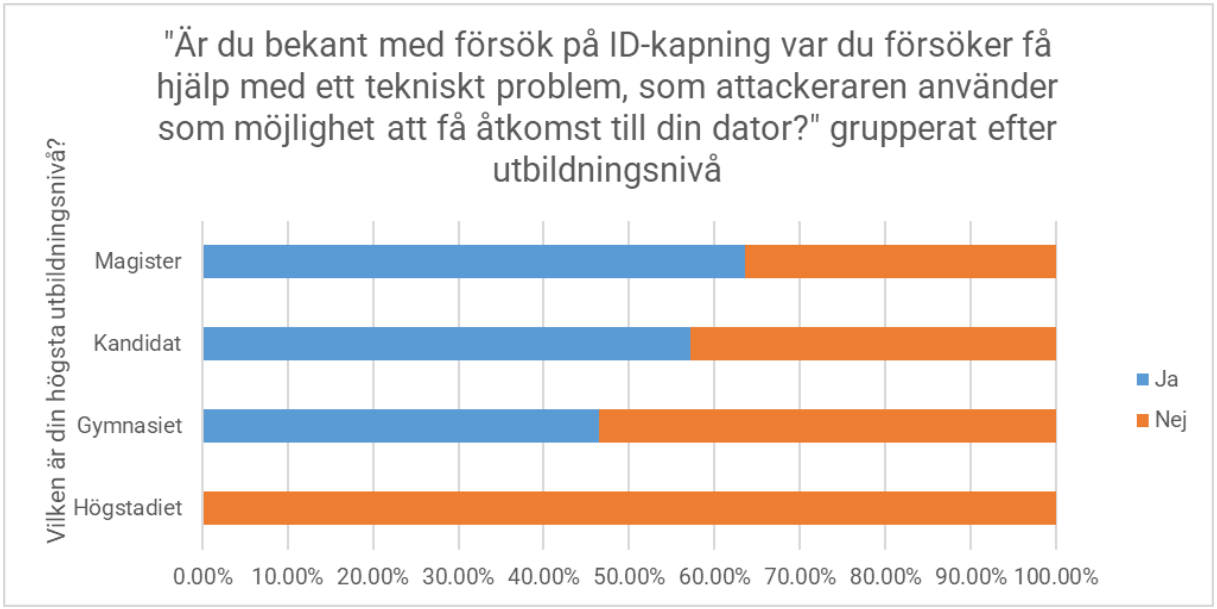


Bild 4.23: Stapeldiagram Fråga 15 grupperat efter utbildningsnivå

Grupperat efter utbildningsnivå så svarade en person med högstadieutbildning att de inte var bekant med denna typ av attack, 26 (46,43%) personer av de med en gymnasieutbildning svarade att de var bekanta med den medan 30 (53,57%) personer svarade att de inte var det. 24 (57,14%) personer av de som var på en kandidatutbildningsnivå svarade att de var bekanta med denna typ av attack. 18 (42,86%) respondenter svarade att de inte var det. Utav de som hade magister som högsta utbildningsnivå så var 7 (63,64%) personer bekanta med denna typ av attack, medan 4 (36,36%) inte var det.

5 Diskussion

Kapitlet inleds med en diskussion kring det tre olika attackerna som tas upp i enkäten. Diskussionen fortsätter sedan med att kolla på respondenternas internetvanor kopplat till ID-kapning och även deras vardagliga teknologier. Detta följs upp med en diskussion kring betydelsen av att arbeta med IT samt utbildningsnivåns och medvetenheten av social engineering attacker. Detta kapitel avslutas med diskussion kring onlinebeteende kring säkerhet för privatpersoner samt applicering av social engineering Hook. I diskussionen kopplas den beskrivna litteraturen samman med vår undersökning för att kunna föra en diskussion.

5.1 Medvetenheten av social engineering attacker

De tre typer av social engineering attacker som inkluderas i enkäten är olika kombinationer av social engineering typer (Krombholz m. fl., 2015). Den första attacken som frågas om är attacken Krombholz m. fl. (2015) beskriver som en waterholing attack, vilket i vår enkät förklaras som när du besöker en hemsida som visar sig inte vara en riktig hemsida. Ungefär 74% av respondenterna var medvetna om denna attack. Den andra attacken är en så kallad phishing attack, när någon försöker få dig att besöka en länk (Conteh & Schmick, 2016). Den tredje är en av typen reverse social engineering, som Gragg (2002) och Conteh & Schmick (2016) beskriver är en attack som innebär att du söker för hjälp med ett tekniskt problem och på så sätt får obehöriga tillgång till personlig information. Trots att Krombholz m. fl. (2015), Conteh & Schmick (2016) och Gragg (2002) beskriver de tre attackerna på ett väldigt likvärdigt sätt så ser vi stora skillnader i vilka attacker som blir igenkända bland respondenterna. Särskilt typen reverse social engineering, som endast 52% av respondenter var bekanta med, i jämförelse med phishing vilket 95% av respondenterna var bekanta med. Detta tyder på att det finns ett stort behov för mer utbildning av vissa attacker. Utbildning är det bästa sättet att motarbeta attacker under kategorin socio-tekniska attacker, vilket alla tre attackerna delvist tillhör (Krombholz m. fl., 2015). Här ser vi också att det finns nytta med Krombholz m. fl. (2015) mer granulära kategorisering jämfört med den som Ivaturi och Janczewski (2011) samt Atkins och Huang (2013) använder sig av, för att tydligare klargöra för användaren skillnader mellan typer av attacker. Waterholing och phishing är båda attacker som alltid hamnar under person-till-person via media då attackeraren inte spelar en aktiv roll i processen utöver att skapa själva länken eller hemsidan (Ivaturi & Janczewski, 2011). Dock kan till exempel waterholing hamna under både tekniska och sociotekniska beroende på hur attacken ser ut och hur den har anpassats för att nå ut till offret (Krombholz m. fl., 2015). Tydligare kategorisering av attacker gör det lättare för ett potentiellt offer att identifiera vad en attack använder sig av för att uppnå sitt mål. Detta i sin tur skapar större förståelse för potentiella risker med de olika typerna av attacker.

Reverse social engineering är också en typ av attack som är mycket lik den välkända IT-support attacken, bara att den i stället spelar på användarens tillit när de själva ringer upp support för hjälp (Conteh & Schmick, 2016). Att denna typ av attack har ett så relativt sett låg bekantskap bland respondenterna kan bero på att den inte är lika vanlig i diskussionen om dessa typer av attacker.

Att 90 % av svenska befolkningen som använder internet, enligt Internetstiftelsen (2021), känner oro för att bli utsatta för bedrägeri är en hög siffra. I och med att oron är hög så kan

man tänka att de ska återspegla sig i den medvetenheten vi ser i olika attacker som just utsätter en person för ID-kapning. Detta kan vi se i hög utsträckning i social engineering attacken phishing, något mindre i attacken waterholing och inte så mycket i attacken reverse social engineering.

Jämför vi resultatet med den medvetenhetsmodell som Arisya m. fl. (2020) presenterar ser vi att phishing attacken går under kategorin bra/hög medvetenhet. Waterholing går under kategorin medel och reverse social engineering under kategorin dålig/låg medvetenhet.

Ett intressant mönster som dyker upp i svaren är också att alla som inte var bekanta med en attack svarade att de inte heller hade råkat ut för en sådan attack, även efter de hade möjligheten att läsa den information om attacken som vi inkluderade i enkäten. Detta tyder på att respondenterna som inte kunde känna igen typerna av attack kan vara i riskzonen för social engineering attacker. Det visar hur viktigt det är att utbilda och att göra användare medvetna kring dessa typer av attacker för att göra det möjlig för personer att skydda sig (Krombholz m. fl.,2015; Jaeger 2018; Grassegger & Nedbal 2021).

5.2 Privatpersoners inställning till ID-kapning

De yngre tenderar att känna mindre oro för att bli utsatta för nätbedrägeri (Internetstiftelsen, 2021). Även i kategorierna ”känner stor oro” och ”känner mycket stor oro” så ligger de yngre åldersgrupperna på en lägre nivå av oro än de äldre åldersgrupperna (Internetstiftelsen, 2021). Resultaten av bekvämlighet med det teknologier som respondenterna använder, ser vi en trend att de yngre åldersgrupperna är mer bekväma i jämförelse med de äldre. Det kan bero på att yngre personer är uppväxta och vana vid de vardagliga teknikerna mer än äldre åldersgrupper. De kan även ge en förklaring till att de yngre känner mindre oro för att de känner sig bekväma med teknologin. Vi ser även att de yngre enligt Internetstiftelsen (2021) är minst drabbade av nätbedrägeri och det kan leda till en ökad känsla av trygghet och bekvämlighet, vilket i sin tur leder till en minskad oro.

Internetstiftelsen (2021) har tittat närmare på orsakerna bakom oron och hur det kan leda till att personer undviker e-tjänster. Oron grundar sig i att de är rädda för att deras personuppgifter ska tas av någon, att de ska bli hackade enligt Internetstiftelsen (2021) och med andra ord utsatta för en ID-kapning (Reyns, 2013; Irvin-Erickson & Ricks, 2019). Det finns även en oron för shopping online och aktiviteter kopplade till internetbank (Internetstiftelsen, 2021; Choi, Kruis, Choo, 2021). Den vanligaste orsaken till ID-kapning är enligt Irvin-Erickson & Ricks (2019) ekonomiska vinningar och därför kan rädslan för att lämna ut sina konto- och kortuppgifter vara stor. Rädslan för säkerheten vid online betalning uppges vara på 41% enligt (European Commission, 2020). I Hille, Walsh och Cleveland (2015) teori om Fear of Identity theft är ekonomiska förluster även en stor del. Det finns även andra konsekvenser som inte är ekonomiska såsom psykiska, fysiska och sociala som kan leda till en ökad oro för att utsättas för en ID-kapning (Irvin-Erickson & Ricks, 2019; Golladay & Holtfreter, 2016). Genom att använda internet för bankverksamheter, ökar risken att bli utsatt för en ID-kapning med 50% och användande av e-handel ökar det med 30% (Reyns, 2013). Även kommunikationsaktiviteter online leder till en ökad risk för social engineering attacker och därmed risk för ID-kapning (Mesch & Dodel 2018). Är riskerna högre vid dessa onlineaktiviteter leder det även till en hög oro för användning av dessa. Reyns (2013) poängterar dock att det inte går att utesluta sig helt från dessa tjänster som vissa enligt Internetstiftelsen (2021) rapport gör på grund av rädsla och oror. I stället tas vikten av utbildning kring användandet av internet upp för att lära

sig skydda sig mot ID-kapningar och på så sätt minska oron (Reyns, 2013; Jaeger 2018). Bankverksamheten, e-handel och kommunikation online kan ses som vanliga teknologier som många använder sig av. På grund av hur vanliga dessa teknologier är så leder det till en ökad risk; detta må vara en förklaring till den höga oron som finns bland svenska internetanvändare idag.

Vid de olika attackerna ser vi att oavsett hur komfortabla respondenten är med tekniken som används så påverkar det inte utsattheten eller försöken av en social engineering attack i någon riktning. Det syns heller inte någon skillnad att de som är mer bekväma med teknologin, har en högre medvetenhet än de som ansåg sig vara mindre bekväma. Det finns dock andra kategorier som ger skillnad i medvetenhet och dessa diskuteras nedan.

5.3 Betydelsen av att arbeta med IT

Analyserar vi svaren uppdelat efter om respondenten jobbar med IT eller inte så kan vi se skillnader på svaren i frågorna kring om man är bekant med försök på ID-kapning, vid det tre olika attackerna. Vid frågan om ID-kapning vid besök av en länk, det vill säga phishing, svarar totalt ca 95% att de är bekanta med den typen. I denna fråga ser vi i princip ingen skillnad mellan de som arbetar med IT och inte. De som inte jobbar inom IT är lite mer än 94% bekanta och den gruppen som jobbar med IT är lite över 95% bekanta.

Vid frågan om bekantskap med försökt på ID-kapning vid besök av en hemsidan, vilket speglar attacker waterholing, så är det lite större skillnad. Totalt sett uppger ca 74% vara medvetna kring denna attack. Det är ca 70% av de som inte jobbar med IT som är bekanta med attacken och ca 86% av de som arbetar med IT som är bekanta.

Störst skillnad syns det på ID-kapningar kopplat till tekniska problem i attacken reverse social engineering. Av alla respondenter är ca 52% bekanta med denna attack. De som inte jobbar med IT, svara ca 43% att de är medvetna och inom IT-arbetande gruppen så är ca 86% bekanta. En förklaring till detta kan kopplas till Jaeger (2018) teori kring information security awareness (ISA) på den individuella nivån. Allmän vetenskap kring informationssystem, vilket vi antar att de som arbetar med IT har i större grad jämfört med de som inte arbetar med IT, har visat sig ge en högre grad ISA (Jaeger, 2018). Både Jaeger (2018) och Grassegger och Nedbal (2021) visar på att ISA har positiv inverkan för agerandet för att skydda sig mot social engineering attacker.

Medvetenhet ökar genom utbildningar inom cybersecurity enligt Muhirwe och White (2016). De som arbetar inom IT-branschen har en högre sannolikhet att ta del av dessa utbildningar då säkerhet inom organisationer också krävs. På så sätt får de utbildning inom cybersecurity som ökar deras medvetenhet och kunskap kring social engineering attacker som de även kan använda privat. Utbildning, träning och medvetenhet är tre faktorer som Hamoud och Aïmeur (2020) visar leder till ett säkrare beteende online. Dessa tre får personer som jobbar inom IT-branschen i högre grad via sitt arbete än de som jobbar inom andra branscher och på så sätt kan de bli med medvetna om social engineering attacker och undvika risker online.

Generellt sätt så har det två sistnämnda attackerna (waterholing och reverse social engineering) en lägre medvetenhet än phishing, vilket var den mest bekanta attacken hos respondenterna. En förklaring på detta kan vara den sociala-miljönivån av ISA (Jaeger, 2018). Det innebär att media lyfter säkerhetsfrågor och problem kring säkerhet och på så sätt ökar ISA hos

individer (Jaeger, 2018). Samhället tar upp attacker och väcker intresse och förståelse kring denna och på så sätt ser vi en högre bekantskap på phishing attacker än waterholing och reverse social engineering. En högre grad av ISA det vill säga ett högre medvetenhet av informationssäkerhet ökar handlandet hos privatpersoner som stödjer säkerheten (Jaeger, 2018; Jaeger & Eckhardt, 2021; Grassegger & Nedbal, 2021).

5.4 Utbildningsnivå kopplat till medvetenheten

Kollar vi på utbildningsnivå kopplat till respondenternas medvetenhet till ID-kapningar genom olika attacker så kan vi se en tydlig trend att de som har högre utbildningsnivå generellt är mer medvetna om ID-kapning kopplat till olika attacker. Utbildningsnivån högstadiet kommer inte diskuteras då den gruppen endast bestod av en respondent. ID-kapningar vid en phishing attack, är 100% av magisterrespondenterna bekanta med, ca 93% av de kandidatutbildade och ca 95 % av de med gymnasiet som högsta utbildning. Alla ligger på en hög procent men en liten skillnad syns.

Waterholing attack är ca 91% av magister gruppen bekanta med, ca 79% av kandidatnivån och ca 66% av gymnasienivån. I denna attack var trenden mer tydlig att högre utbildningsnivå ger större medvetenhet om attackerna.

Den sista attacken reverse social engineering visar även på denna trend. Magisternivån har högst medvetenhet med ca 64% av respondenterna. Inom kandidatnivån uppger ca 57% sig vara bekanta med denna attack och ca 46% av gruppen med utbildning på gymnasienivå.

Internetstiftelsen (2021) visar att de med grundskoleutbildning känner en högre "stor oro" (47%) kring bedrägeriförsök online medan högskoleutbildade känner "stor oro" i något lägre grad (42%). Det finns enligt Brands and van Wilsem (2021) en lägre nivå av rädsla bland högutbildade och även hos höginkomsthushåll. Detta kan eventuellt kopplas till att de mer högutbildade känner mindre oro för att de är med medvetna om ID-kapningar och hur en attack kan gå till. Varför medvetenheten är högre bland högutbildade kan bero på att högre utbildningar diskuterar IT-säkerhet mer, vilket då leder till en ökad medvetenhet (Kumar, Chaudhary & Kumar, 2015). Dock bland de som har blivit utsatta av eller försök till ID-kapning är det endast 26% av de med grundskoleutbildning, medan 49% av de med högskoleutbildning (Internetstiftelsen, 2021). Det går dock inte att veta vilken del som är "utsatt för" eller vilken del som bara är "försök" till en ID-kapning. En möjlig förklaring kan även vara om medvetenheten är låg bland de med längre utbildning så är de inte medvetna om att de har blivit utsatt för eller försökt till en ID-kapning och därför skiljer sig procenten mellan utbildningsnivåerna. Likaså säger Mesch och Dodel (2018) att det är de med lägre utbildningsnivå som har en högre sannolikhet att agera på bedrägeriförsök. Detta stämmer mer överens med att medvetenheten hos de längre utbildningsnivåerna är längre, för att de inte har kunskap kring det och det ger även en förklaring till att de känner en större oro för att utsättas.

Utbildning inom säkerhet online är något som både Muhirwe och White (2016) och Hamoud och Aïmeur (2020) vill se i en högre grad. Muhirwe och White (2016) tycker att många aktiviteter sker online och då ska det finnas utbildning i hur de används på ett säkert sätt, exempelvis i skolans aktiviteter. Medan Muhirwe och White (2016) understryker att de vill se utbildningar om onlineskydd borde startade redan barndomen. Då utbildningar har en påverkan på beteendet och medvetenheten, som i sin tur har en påverkan på medvetenhet kan detta leda till en ökad medvetenhet i framtiden. De kan även leda till att antalet lyckade social

engineering attacker bli färre och så även antalet ID-kapningar. Det kan leda till en mindre klyfta mellan de som arbetar inom IT-branschen eller inte och även på utbildningsnivåerna i framtiden om alla får en grundläggande utbildning i en lägre ålder. Salam, Dai och Wang (2021) påstår att det har blivit ett kritiskt problem för samhället och det ser vi även i MySafety (2021) rapport om att antalet attacker och försök ökar samt Hamoud och Aïmeur (2020) som säger att det blir allt vanligare med attacker mot människor och deras data. Vi ser även i vår undersökning och enligt Kruger och Kearney medvetenhetsmodell att endast en attack, phishing, ligger på en hög medvetenhetsnivå. Waterholing på en medel och reverser social engineering på en låg nivå. Samtidigt som oron ligger på en hög nivå där 90% enligt Internetstiftelsen (2021) upplever någon form av oro.

5.5 Onlinebeteende hos privatpersoner

Det är få personer som svarar att de har blivit utsatta för en attack. Endast 5 % i attacken phishing, mindre än 2% i en waterholing attack och samma i reverse social engineering attack. Respondenternas olika beskrivningarna av hur attackerna som de har blivit utsatta för gick till, visar på olika beteenden som kan ha påverkar deras skydd mot en ID-kapning.

En respondent som blivit utsatt för en ID-kapning svarade "…Fick ett sms en vecka senare med Apple som avsändare med en text som sade att telefonen hittats samt en länk till vad jag trodde var riktiga iCloud/Find my iPhone. Blev stressad då jag tänkte att personen som startat telefonen kanske stänger av igen, så jag skyndande att klicka på länken. …". Denna person agerade impulsivt, ett beteende som kan anses vara riskabelt för säkerheten (Irvin-Erickson & Ricks, 2019). Personen var inte medveten om vem som kontaktar denne eller verifierade kontakten, ytterligare beteende som kan öka riskerna för bedragaren att lyckas med en attack (Koyun & Al Janabi, 2017).

I resterande av respondenternas svar kring hur de blivit utsatta för en attack så var orsaken bakom flera ID-kapningar att de inte visste vem som tar kontakt och dålig verifieringen av kontakten. Detta är ett beteende som Koyun & Al Janabi (2017) förklarar att vara uppmärksam på, för att minska riskerna för en att bli utsatt för en attack och få sin ID kapad. Det går även att förknippa med beteendet om att vara försiktig med att öppna meddelande från okända avsändare (Irvin-Erickson & Ricks, 2019) eller att uppmärksamma konstig eller ovanlig avsändare som Gretizer m. fl. (2014) nämner.

I attacken phishing hade ca 63% svarat att de har undvikit en sådan attack, vilket utgör en majoritet av de som var medvetna om attacken. Waterholing var det ca 23% som undvikit den attacken och ca 14% vid en reverse social engineering attack. Detta speglar medvetenheten på alla tre attacker som tidigare diskuterats. Här syns även en skillnad i bland annat method of distribution som Heartfield & Loukas (2015) diskuterar, i hur den mindre komplicerade attacken har en bredare målgrupp för att kompensera för den lägre effekten. Medans de attacker som skapar en starkare relation med offret, det vill säga har en mycket lägre grad av automation, också når ut till färre (Heartfield & Loukas, 2015).

Vid granskning av svaren på frågorna till vad det var som gjorde att man undvek en attack finns det flera vanliga anledningar. Indikationer på en attack, som tas upp av Koyun & Al Janabi (2017) och Gretizer m. fl. (2014), som vi även ser ett stort antal av respondenternas sätt att undvika attacken på, var att det såg konstig eller inte rätt ut. Detta var den vanligaste anledningen hos respondenterna till varför de undvek en attack.

Respondenterna var även uppmärksamma på dålig grammatik, något som indirekt ingår i svarsalternativet det såg konstigt eller inte rätt ut, vilket nämns av Gretizer m. fl. (2014) som en tydlig indikation på social engineering försök. Vid en misstanke om en attack så ska man inte agera enligt Koyun & Al Janabi (2017). Vid de respondenter som svarade att det inte uppfyllde förväntningarna när en eventuell attack påbörjats (antingen kommunikation med support eller efter att de klickat på länken) avsluta de agerandet direkt, för att undvika en attack likt Koyun & Al Janabi (2017) beskrivning. Ytterligare en faktor som tas upp av Koyun & Al Janabi (2017) är att tänka efter om det är för bra för att vara sant, detta uppgav respondenterna som en anledning till att de undvek en eventuell social engineering attack. Dessa tre svarsalternativ var alla ungefär lika vanligt förekommande som anledning till att de undvek en attack. Det var ungefär hälften så förekommande jämfört med den vanligaste. Kollar vi på det specifika attackerna och det mest förekommande svaret för att undvika en attack, var det olika på alla tre. Generellt så var anledningarna mycket varierande på alla attacker.

5.6 Applicering av Social Engineering Hook

När man applicerar teorin social engineering hook på det resultat som vi har fått in i våran studie så ser vi ett sätt att kategorisera attackerna efter hur de olika stegen ser ut för just den attacken. Hook, eller orchestration, som beskrivs av Conteh & Schmick (2016), Koyun & Al Janabi (2017) och Heartfield & Loukas (2015), påverkar till stor grad hur många attacken når ut till. De attacker som når ut till många såsom phishing attacker är inte så komplicerade attacker men som ändå är effektiva, medans de attacker med en mycket högre grad av automation som beskrivet av Heartfield & Loukas (2015) är också attacker som inte gör anspel på offrets svagheter till samma grad som en attack med en mindre grad av automation.

I sin beskrivning av reverse social engineering förklarar Gragg (2002) hur attackeraren använder sig av tillit som byggs mellan attackeraren och offret efter att en reverse social engineering attack sker, och denna typ av attack är ett exempel på en attack som använder sig av en mer personlig koppling under exploitation steget, som diskuterat av Salahdine & Kaabouch (2019), Koyun & Al Janabi (2017), Conteh & Schmick (2016) och Heartfield & Loukas (2015). Denna typ av attack har också möjlighet för ett execution steg med flera upprepningar då offret litar på attackeraren som beskrivet av Salahdine & Kaabouch (2019) och Heartfield & Loukas (2015). Kombinera effekten av den typ av attack som använder sig av en deception vector (Heartfield & Loukas, 2015) som spelar på offrets beteende direkt (Krombholz m. fl., 2015, Conteh & Schmick, 2016) med att de typerna av attacker är mindre bekanta hos dem som har svarat på enkäten så syns det en tydlig svaghet som skulle kunna utgöra ett hot för privatpersoner.

6 Slutsats

I detta kapitel avser vi att besvara studiens forskningsfråga:

Hur medvetna anser sig svenska internetanvändare vara om social engineering attacker och hur det kan leda till en ID-kapning?

De social engineering attacker vi valde att kolla närmre på är waterholing, phishing och reverse social engineering. Det är tre vanliga former av attacker som kan användas för att komma åt känslig information från privatpersoner (Krombholz m. fl., 2015).

Medvetenheten för attackerna ser olika ut beroende på vilken attack det är. Medvetenheten om ID-kapning vid besök av en falsk länk, det vill säga en phishing attack var hög, ca 95%. Medvetenheten av ID-kapning vid besök av en falsk hemsida, det som heter waterholing var medvetenheten medelhög i form av ca 74%. I frågan om ID-kapning vid teknisk support, som motsvarar attacken reverse social engineering så var medvetenheten lägre än de andra med ca 52 %. I och med oron för nätbedrägeri var så pass hög som 9 av 10 personer (Internetstiftelsen, 2021), så borde även det synas i medvetandet av ID-kapning genom olika social engineering attacker.

Privatpersoners arbete och utbildning påverkade medvetenheten. De som arbetar med IT har en högre medvetenhet angående alla attacker än de som inte arbetar med IT. Utbildning om attackerna är en avgörande faktor för att kunna identifiera och förhindra att bli utsatta för dem (Krombholz m. fl., 2015). Här ser vi även en betydelse av information security awareness (ISA) och att de leder till högre medvetenhet (Jaeger, 2018; Grassegger och Nedbal, 2021; Jaeger och Eckhardt, 2021). Högre utbildning visade även vara en faktor som ledde till högre medvetenhet. Det visade att de med en utbildning på magisternivå hade något högre medvetenhet på alla attacker än de på kandidatnivå och den utbildningsnivå med lägst medvetenhet var de som har gymnasiet som utbildningsnivå.

De yngre känner sig mer bekväma med sin dagliga teknologi än de äldre. I det olika åldersgrupperna ser vi en mycket stor oro för ID kapningar i äldre åldersgrupper men den minskar för varje yngre åldersgrupp (Internetstiftelsen, 2021).

Slutligen så när de kommer till privatpersoner beteende vid onlineaktiviteter ser vi att de är medvetna om att vara uppmärksamma om en länk / hemsida ser annorlunda ut och även på dålig grammatik. De är även försiktiga i sitt agerande när något ser ut att vara för bra för att vara sant och använder då sunt förnuft för att undvika risken för en ID-kapning. Beteendet kring att inte verifiera kontakten eller kolla avsändaren var det som enligt vår undersökning i störst utsträckning ledde till att en attack lyckades.

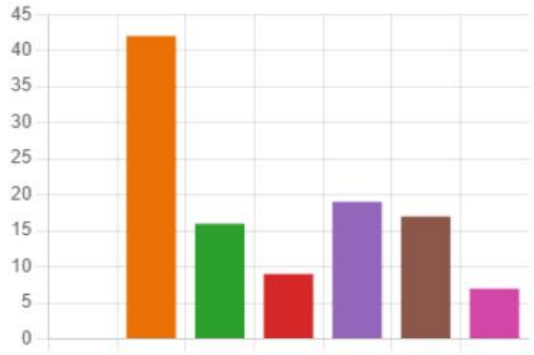
Appendix

IT-attacker mot dig som privatperson

110	03:02	Closed
Responses	Average time to complete	Status

1. Hur gammal är du?

Under 18	0
18-24	42
25-30	16
31-40	9
41-50	19
51-60	17
61+	7



2. Vilken är din högsta utbildningsnivå?

Högstadiet	1
Gymnasiet	56
Kandidat	42
Magister	11

3. Arbetar du inom IT-branschen?

Ja	22
Nej	88

4. Hur bekväm skulle du säga att du är med den teknologi du använder dig av i vardagen?

110
Responses

4.16
Average Number

5. Är du bekant med försök på ID-kapning där du besöker en hemsida som inte visar sig vara den riktiga hemsidan?

Ja	81
Nej	29

6. Har du råkat ut för en sådan attack?

Ja	2
Ja, men jag undvek attacken	25
Nej	83

7. Hur länge sedan var detta?

1-12 månader sedan	0
1-3 år sedan	0
3-5 år sedan	0
5+ år sedan	2

8. Beskriv attacken om du vill (Exempelvis vilken hemsida det skedde på? Hur du hamnade på sidan?)

1
Responses

Latest Responses

9. Vad var det som gjorde att du undvek attacken?

Felaktig address till hemsida	9
Dålig grammatik	1
För bra för att vara sant	3
Hemsidan såg inte riktigt rätt ut...	10
Other	2

10. Är du bekant med försök på ID-kapning där någon försöker få dig att besöka en länk?

Ja	104
Nej	6

11. Har du råkat ut för en sådan attack?

Ja	6
Ja, men jag undvek attacken	69
Nej	35

12. Hur länge sedan var detta?

1-12 månader sedan	5
1-3 år sedan	0
3-5 år sedan	1
5+ år sedan	0

13. Beskriv attacken om du vill (Exempelvis var fick du länken? Var du stressad? Vad hände när du klickade?)

4
Responses

Latest Responses

14. Vad var det som gjorde att du undvek attacken?

Länken såg inte rätt ut	32
Dålig grammatik	17
För bra för att vara sant	13
Efter jag tryckte på lanken var d...	2
Other	5

15. Är du bekant med försök på ID-kapning var du försöker få hjälp med ett tekniskt problem, som attackeraren använder som möjlighet att få åtkomst till din dator?

Ja	57
Nej	53

16. Har du råkat ut för en sådan attack?

Ja	2
Ja, men jag undvek attacken	15
Nej	93

17. Hur länge sedan var detta?

1-12 månader sedan	0
1-3 år sedan	2
3-5 år sedan	0
5+ år sedan	0

18. Beskriv attacken om du vill (Exempelvis vilken typ av problem var det som krävde support? Vad för support fick du?)

1
Responses

Latest Responses

19. Vad var det som gjorde att du undvek attacken?

Länken till support såg inte rätt ut	2
Dålig grammatik	3
För bra för att vara sant	1
Kommunikationen var inte som ...	7
Other	2

20. Använder du dig av BankID

Ja	109
Nej	1

21. Känner du att du kan lita på BankID?

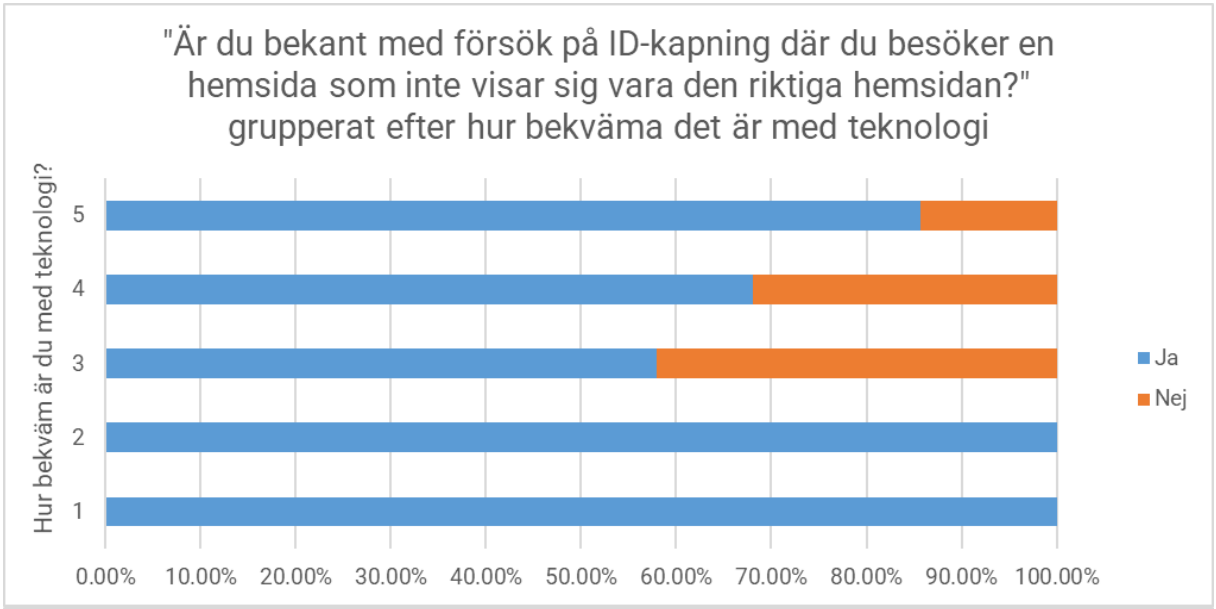
110
Responses

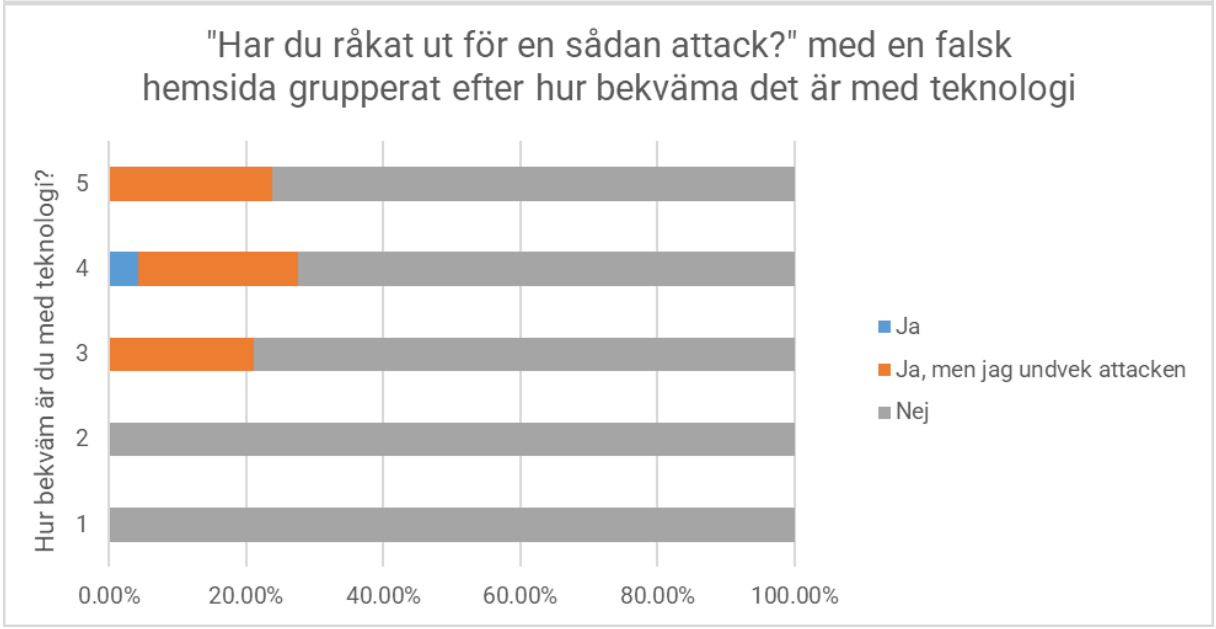
4.35
Average Number

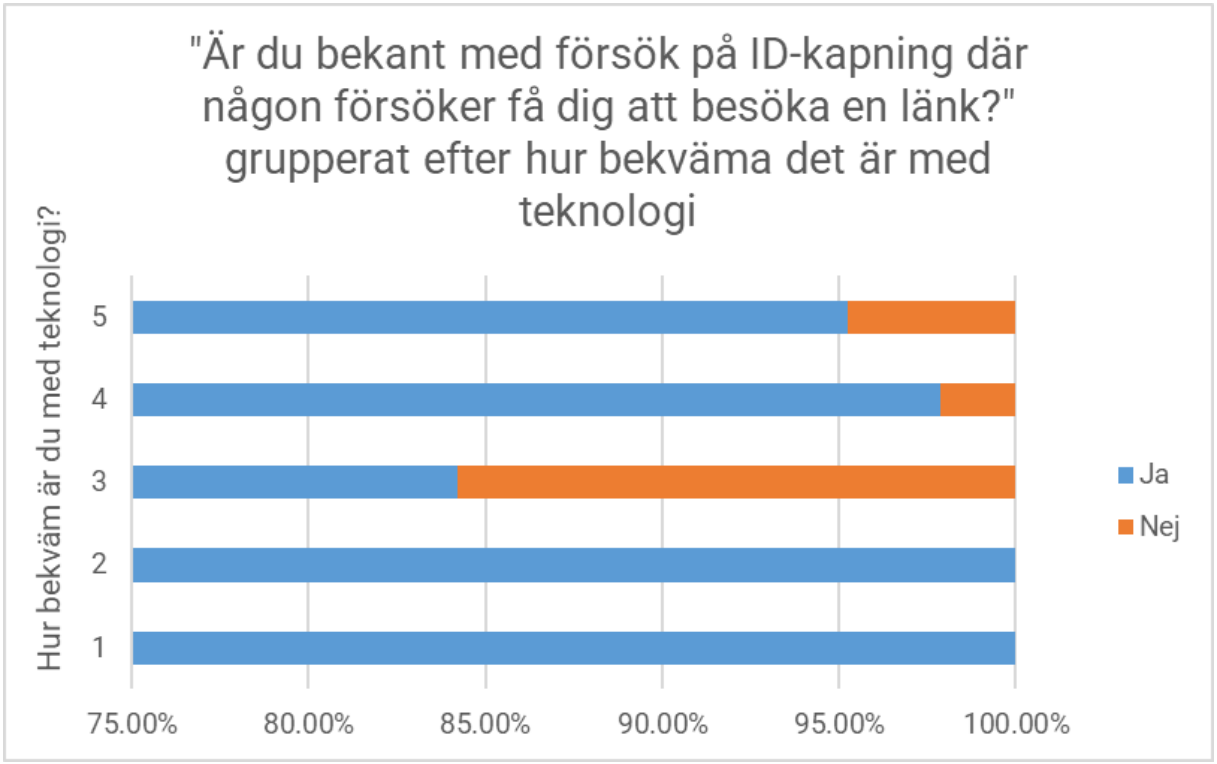
22. Tycker du Bank-ID gör tillräckligt för att skydda dig från bedrägeri försök?

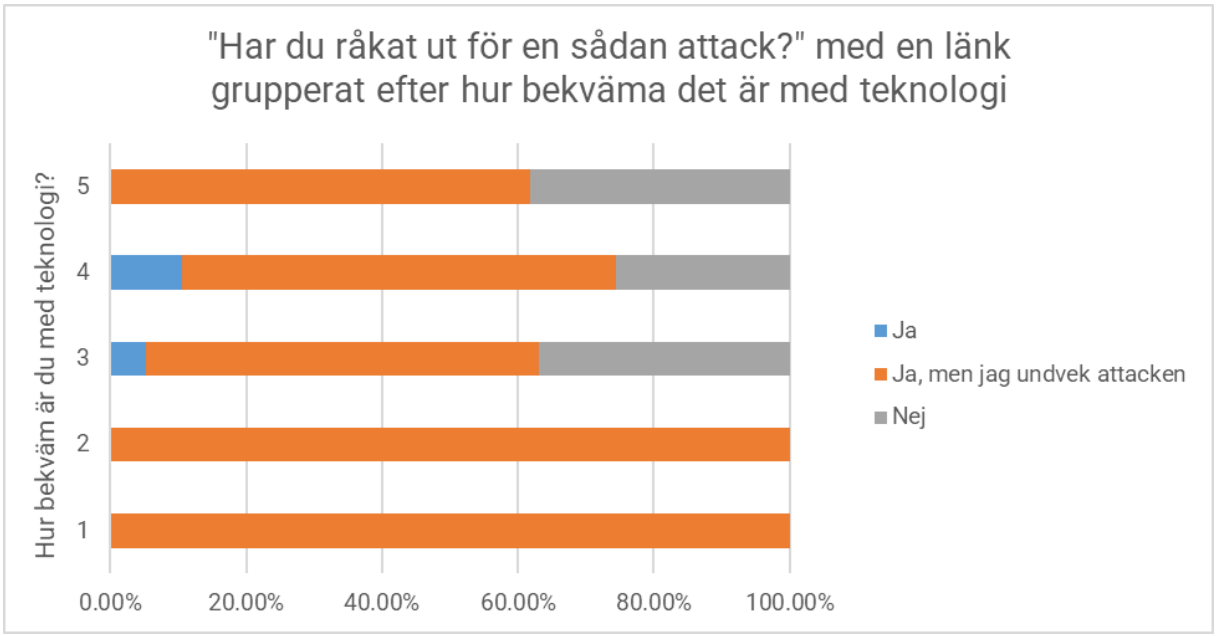
110
Responses

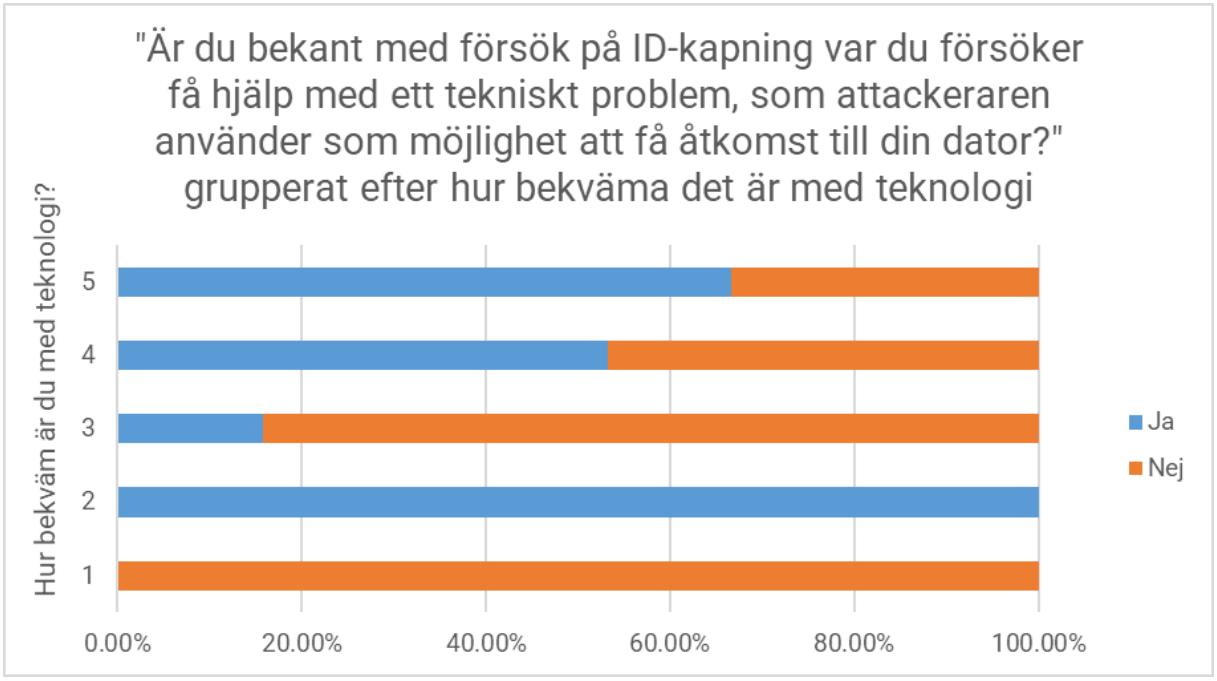
3.80
Average Number


"Är du bekant med försök på ID-kapning där du besöker en hemsida som inte visar sig vara den riktiga hemsidan?" grupperat efter hur bekväma det är med teknologi
Hur bekväm är du med teknologi?
5
4
3
2
1
0.00%
10.00%
20.00%
30.00%
40.00%
50.00%
60.00%
70.00%
80.00%
90.00%
100.00%
Ja
Nej

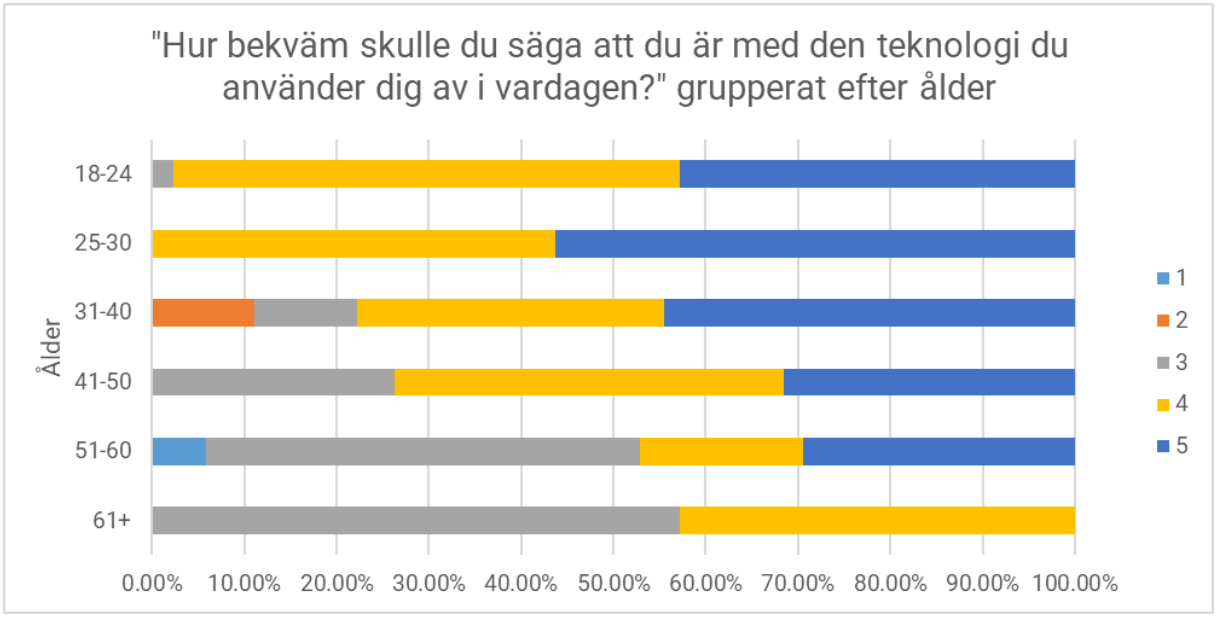

"Har du råkat ut för en sådan attack?" med en falsk hemsida grupperat efter hur bekväma det är med teknologi
Hur bekväm är du med teknologi?
5
4
3
2
1
0.00%
20.00%
40.00%
60.00%
80.00%
100.00%
Ja
Ja, men jag undvek attacken
Nej


"Är du bekant med försök på ID-kapning där någon försöker få dig att besöka en länk?" grupperat efter hur bekväma det är med teknologi
Hur bekväm är du med teknologi?
5
4
3
2
1
75.00%
80.00%
85.00%
90.00%
95.00%
100.00%
Ja
Nej


"Har du råkat ut för en sådan attack?" med en länk grupperat efter hur bekväma det är med teknologi
Hur bekväm är du med teknologi?
5
4
3
2
1
0.00%
20.00%
40.00%
60.00%
80.00%
100.00%
Ja
Ja, men jag undvek attacken
Nej


"Är du bekant med försök på ID-kapning var du försöker få hjälp med ett tekniskt problem, som attackeraren använder som möjlighet att få åtkomst till din dator?" grupperat efter hur bekväma det är med teknologi
Hur bekväm är du med teknologi?
5
4
3
2
1
0.00%
20.00%
40.00%
60.00%
80.00%
100.00%
Ja
Nej


"Har du råkat ut för en sådan attack?" när respondenten ringer upp support grupperat efter hur bekväma det är med teknologi
Hur bekväm är du med teknologi?
5
4
3
2
1
0.00%
20.00%
40.00%
60.00%
80.00%
100.00%
Ja
Ja, men jag undvek attacken
Nej


"Hur bekväm skulle du säga att du är med den teknologi du använder dig av i vardagen?" grupperat efter ålder
Ålder
18-24
25-30
31-40
41-50
51-60
61+
0.00% 10.00% 20.00% 30.00% 40.00% 50.00% 60.00% 70.00% 80.00% 90.00% 100.00%
1
2
3
4
5

Referenser

Arisya, K. F., Ruldeviyani, Y., Prakoso, R., & Fadhilah, A. L. (2020). Measurement of Information Security Awareness Level: A Case Study of Mobile Banking (M-Banking) Users. In *2020 Fifth International Conference on Informatics and Computing (ICIC)* (pp. 1-5). Tillgänglig online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9288516 [Hämtad 21 Juni 2022]

Atkins, B. and Huang, W., 2013. A study of social engineering in online frauds. *Open Journal of Social Sciences*, 1(03), p.23. Tillgänglig online: https://www.scirp.org/html/36435.html [Hämtad 16 Augusti 2022]

Brands, J., & van Wilsem, J. (2021). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*, 18(2), pp. 213-234. Tillgänglig online: https://journals.sagepub.com/doi/pdf/10.1177/1477370819839619 [Hämtad 10 Juni 2022]

Conteh, N.Y. and Schmick, P.J., 2016. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6(23)*, p.31. Tillgänglig online: https://www.researchgate.net/profile/Nabie-Conteh-2/publication/294421084_Cybersecurityrisks_vulnerabilities_and_countermeasures_to_prevent_social_engineering_attacks/links/56e2733408aebc9edb19eebc/Cybersecurityrisks-vulnerabilities-and-countermeasures-to-prevent-social-engineering-attacks.pdf?_sg%5B0%5D=started_experiment_milestone&origin=journalDetail [Hämtad 11 Augusti 2022]

European Commission, 2020. Europeans' attitudes towards cyber security (cybercrime). Tillgänglig online: https://europa.eu/eurobarometer/surveys/detail/2249 [Hämtad 18 Juni 2022]

Gragg, D., 2003. A multi-level defense against social engineering. *SANS Reading Room, 13*, pp.1-21. Tillgänglig online: http://taupe.free.fr/book/psycho/social%20engineering/Social%20Engineering%20-%20Sans%20Institute%20-%20Multi%20Level%20Defense%20Against%20Social%20Engineering.pdf [Hämtad 11 Augusti 2022]

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science, 181*, pp. 59-

66. Tillgänglig online: https://www.sciencedirect.com/science/article/pii/S1877050921001381 [Hämtad 18 Juni 2022]

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014, May). Analysis of unintentional insider threats deriving from social engineering exploits. In 2014 *IEEE Security and Privacy Workshops* (pp. 236-250). Tillgänglig online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6957309 [Hämtad 12 Juni 2022]

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, 12(5), pp. 741-760. Tillgänglig online: https://www.tandfonline.com/doi/pdf/10.1080/15564886.2016.1177766?needAccess=true [Hämtad 18 Juni 2022]

Hamoud, A., & Aïmeur, E. (2020). Handling user-oriented cyber-attacks: STRIM, a user-based security training model. *Frontiers in Computer Science.* Tillgänglig online: https://www.frontiersin.org/articles/10.3389/fcomp.2020.00025/full [Hämtad 15 Juni 2022]

Heartfield, R. and Loukas, G. (2015) A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks, *ACM Computing Surveys (CSUR), 48(3)*, pp. 1–39. Tillgänglig online: http://dx.doi.org.ludwig.lub.lu.se/10.1145/2835375 [Hämtad 11 Augusti 2022]

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, 30, pp. 1-19. Tillgänglig online: Tillgänglig genom: LUSEM Library website https://www.lusem.lu.se/library [Hämtad 15 Juni 2022]

Internetstiftelsen (2021) Svenskarna och internet 2021. Tillgänglig online: https://svenskarnaochinternet.se/app/uploads/2021/09/internetstiftelsen-svenskarna-och-internet-2021.pdf [Hämtad 9 Maj 2022]

Irvin-Erickson, Y., & Ricks, A. (2019). Identity theft and fraud victimization: What we know about identity theft and fraud victims from research-and practice-based evidence. Tillgänglig online:

https://ncvc.dspacedirect.org/bitstream/handle/20.500.11990/1544/CVR%20Research%20Syntheses_Identity%20Theft%20and%20Fraud_Report.pdf?sequence=1&isAllowed=y [Hämtad 14 April 2022]

Ivaturi, K. & Janczewski, L. (2011) A Taxonomy for Social Engineering attacks CONF-IRM 2011 Proceedings. 15. Tillgänglig online: https://aisel.aisnet.org/confirm2011/15 [Hämtad 11 Augusti 2022]

Jaeger, L. (2018). Information security awareness: literature review and integrative framework. In *Proceedings of the 51st Hawaii International Conference on System Sciences.* Tillgänglig online: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1647&context=hicss-51 [Hämtad 11 April 2022]

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, 31(3), pp. 429-472. Tillgänglig online: https://onlinelibrary.wiley.com/doi/full/10.1111/isj.12317?casa_token=oekUU5mHn_4AAAAA%3Al2M1eZwY94tJFGjnjs-NcFcDu9TXNSmSGyqML0RjhkgYKAwjlZCYqemdRIDqDFfkh4ST9Jl_SxB_h7Q [Hämtad 14 Juni 2022]

Jain, A., Tailang, H., Goswami, H., Dutta, S., Sankhla, M. S., & Kumar, R. (2016). Social engineering: Hacking a human being through technology. *IOSR Journal of Computer Engineering*, 18(5), pp. 94-100. Tillgänglig online: https://www.researchgate.net/profile/Rajeev-Kumar-5/publication/309234725_Social_Engineering_Hacking_a_Human_Being_through_Technology/links/5806568908aeb85ac85f4742/Social-Engineering-Hacking-a-Human-Being-through-Technology.pdf [Hämtad 14 Juni 2022]

Koyun, A., & Al Janabi, E. (2017). Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, vol. 4, no. 6, pp. 7533-7538. Tillgänglig online: https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf [Hämtad 8 April 2022]

Krombholz, K., Hobel, H., Huber, M., Weippl E. (2015). Advanced social engineering attacks, *Journal of Information Security and Applications*. Vol 22, pp. 113-122. Tillgänglig genom: LUSEM Library website https://www.lusem.lu.se/library [Hämtad 30 Mars 2022] https://www.sciencedirect.com/science/article/pii/S2214212614001343#

Kumar, A., Chaudhary, M., & Kumar, N. (2015). Social engineering threats and awareness: a survey. *European Journal of Advances in Engineering and Technology*, vol. 2, no. 11, pp. 15-19. Tillgänglig online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1075.1678&rep=rep1&type=pdf [Hämtad 8 April 2022]

Mouton, F., Leenen, L. & Venter, H.S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*. Vol. 59, pp. 186-209. Tillgänglig genom: LUSEM Library website https://www.lusem.lu.se/library [Hämtad 23 April 2022] https://www.sciencedirect.com/science/article/pii/S0167404816300268

Muhirwe, J., & White, N. (2016). CYBERSECURITY AWARENESS AND PRACTICE OF NEXT GENERATION CORPORATE TECHNOLOGY USERS. *Issues in Information Systems*, 17(2). Tillgänglig online: https://www.iacis.org/iis/2016/2_iis_2016_183-192.pdf [Hämtad 18 Juni 2022]

MySafety (2021). BEDRÄGERI- OCH ID-KAPNINGSRAPPORTEN. Tillgänglig online: https://www.mysafety.se/sites/default/files/section/mysafety-rapport%20final.pdf [Hämtad 1 April 2022]

Oates, B. (2006). Researching Information Systems and Computing, London: SAGE Publications

Polisen (2021). Id-kapning – skydda dig. Tillgänglig online: https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/bedrageri/identitetsintrang/ [Hämtad 31 Mars 2022]

Randa, R., & Reyns, B. W. (2020). The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the National Crime Victimization Survey. *Deviant Behavior*, 41(10), pp. 1290-1304. Tillgänglig online: https://www.tandfonline.com/doi/pdf/10.1080/01639625.2019.1612980?needAccess=true [Hämtad 11 Juni 2022]

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, vol. 50, no. 2, pp. 216-238. Tillgänlig genom: LUSEM Library website https://www.lusem.lu.se/library [Hämtad 12 April 2022] https://journals-sagepub-com.ludwig.lub.lu.se/doi/pdf/10.1177/0022427811425539 (via lu inloggning)

Salahdine F & Kaabouch N. (2019) Social Engineering Attacks: A Survey. *Future Internet* 11, no. 4: 89. Tillgänglig online: https://www.mdpi.com/1999-5903/11/4/89/htm [Hämtad 6 April 2022]

Salam, A. F., Dai, H., & Wang, L. (2021). Online Users' Identity Theft and Coping Strategies, Attribution and Sense of Urgency: A Non-Linear Quadratic Effect Assessment. *Information Systems Frontiers*, pp. 1-20. Tillgänglig online: https://link.springer.com/article/10.1007/s10796-021-10194-w [Hämtad 26 Juni 2022]

Thornburgh, T. (2004) 'Social engineering', Proceedings of the 1st Annual Conference: Information Security Curriculum Development, pp. 133–135. Tillgänglig genom: LUSEM Library website https://www.lusem.lu.se/library [Hämtad 15 Juni 2022] https://dl-acm-org.ludwig.lub.lu.se/doi/pdf/10.1145/1059524.1059554

Wang, L. H., & Liou, S. (2021, December). How Should I Do? Users' Attitude Toward Information Security and Data Protection Using Smartphone. In *2021 9th International Conference on Orange Technology (ICOT)* (pp. 1-5). Tillgänglig online: https://ieeexplore.ieee.org/abstract/document/9680626 [Hämtad 20 Juni 202