

## EN STUDIE OM HUR VÄL SVENSKA INTERNETANVÄNDARE UPPTÄCKER PHISHING PÅ SVENSKA JÄMFÖRT MED ENGELSKA

## A STUDY ON HOW WELL SWEDISH INTERNET USERS DETECT PHISHING IN SWEDISH COMPARED TO ENGLISH

Examensarbete inom huvudområdet  
Informationsteknologi

Grundnivå nivå 22,5 Högskolepoäng  
IT610G  
Vårtermin 2020

2020-06-15

Rickard Pettersson  
a17ricpe@student.his.se

Handledare: Joakim Kävrestad  
Examinator: Marcus Nohlberg

## **Förord**

Jag vill passa på att tacka min handledare Joakim Kävrestad som varit snabb med att svara på alla mina frågor, vilket var ganska många. Stort tack för all feedback på arbetet och alla tips om statistik!

Jag vill även tacka min examinator Marcus Nohlberg för tydlig och bra feedback som bidrog till att jag kunde göra ett bättre arbete.

Ett stort tack till alla som tog sig tid till att svara på enkäten, utan er hade denna studie inte kunnat genomföras!

Sist men inte minst vill jag tacka mina nära och kära som stöttat och hjälpt mig genom hela utbildningen.

## Abstract

This study has examined a relatively unexplored area of phishing; the impact of language on people's susceptibility to phishing. The purpose of the study was to investigate how big the difference is between how well Swedish Internet users can detect phishing emails in Swedish compared to English. For this purpose, an online questionnaire was created containing 32 emails in both Swedish and English. The 32 emails were divided into four equally large groups based on the type and language of the email. Participants were then asked to categorize the emails as either legitimate or phishing. The target group of the study consisted of Internet users between the ages of 18 and 81 with Swedish as their native language. A quantitative method was applied to the questionnaire, whereupon statistical analyses were used to answer the purpose of the study.

The results of the study show a significant difference ( $p = 0,039$ ) between how well Swedish Internet users detect phishing in Swedish compared to English. The participants incorrectly identified 20% of the English phishing emails and 17% of the Swedish phishing emails as legitimate. This result shows a weak indication that Swedish internet users are better at detecting phishing in Swedish compared to English.

Furthermore, the results strongly indicate that English language skills and IT-competence are important factors when identifying English legitimate emails. There were no signs indicating that those two factors made the participants better at detecting English phishing emails. However, findings in the study suggests that the participants may have used non-language cues to identify the English phishing emails.

*Keywords: Anti-phishing, information security, phishing, survey.*

## Sammanfattning

Denna studie har undersökt ett relativt outforskat område inom phishing; språkets inverkan på människors mottaglighet för phishing. Syftet med studien var att undersöka hur stor skillnaden är mellan hur bra svenska Internetanvändare kan upptäcka phishing-mejl på svenska jämfört med engelska. För detta ändamål skapades en webbenkät med 32 mejl på både svenska och engelska. De 32 mejlen delades in i fyra lika stora grupper baserat på mejlets typ och språk. Deltagarna blev sedan tillfrågade att kategorisera mejlen som antingen legitima eller phishing. Målgruppen för studien bestod av Internetanvändare mellan 18–81 år med svenska som modersmål. En kvantitativ metod tillämpades på frågeformuläret, varpå statistiska analyser användes för att besvara syftet med studien.

Studiens resultat visar en signifikant skillnad ( $p = 0,039$ ) mellan hur väl svenska Internetanvändare upptäcker phishing på svenska jämfört med engelska. Deltagarna identifierade felaktigt 20 % av de engelska phishing-mejlen och 17 % av de svenska phishing-mejlen som legitima. Resultatet visar svaga indikationer på att svenska Internetanvändare är bättre på att upptäcka phishing på svenska jämfört med engelska.

Resultatet i studien visar även starka indikationer på att engelsk språkförmåga och IT-kompetens är betydande faktorer vid identifiering av engelska legitima mejl. Det fanns inga tecken som tyder på att dessa faktorer gjorde deltagarna bättre på att upptäcka engelska phishing-mejl. Däremot tyder resultatet på att deltagarna kan ha nyttjat icke-språkliga ledtrådar till att identifiera de engelska phishing-mejlen.

Nyckelord: *Anti-phishing, enkät, informationssäkerhet, phishing.*

## Innehållsförteckning

1. Introduktion.....	1
2. Bakgrund.....	2
2.1. Vad är phishing.....	2
2.2. Komponenter och metoder inom phishing .....	2
2.3. Phishing – Ett växande problem.....	3
2.4. Tidigare forskning .....	4
3. Problembakgrund.....	7
3.1. Problemområde.....	7
3.2. Avgränsning.....	8
3.3. Mål och förväntat bidrag .....	8
4. Metod .....	10
4.1. Processöversikt .....	10
4.2. Forskningsmål .....	10
4.3. Enkätmetodik.....	11
4.3.1. Kvalitativa och kvantitativa undersökningar.....	11
4.3.2. Standardisering & strukturering .....	12
4.3.3. Frågor och formuleringar .....	12
4.3.4. Population och urval.....	13
4.3.5. Verktyg vid genomförande.....	14
4.3.6. Reliabilitet och validitet .....	14
4.3.7. Etiska överväganden .....	16
4.4. Sammanställning av studiens metod.....	17
4.5. Dataanalys .....	18
5. Resultat .....	20
5.1. Strukturering av insamlade data .....	20
5.2. Deltagare.....	22

5.3.	Åldersfördelning bland deltagarna .....	22
5.4.	Språkförmåga inom engelska .....	23
5.5.	IT-kompetens.....	24
5.6.	Svenska legitima mejl.....	24
5.7.	Engelska legitima mejl .....	25
5.8.	Svenska phishing-mejl.....	27
5.9.	Engelska phishing-mejl .....	28
6.	Analys och slutsats.....	31
6.1.	Analys av insamlade data .....	31
6.1.1.	Analys av IT-kompetens .....	31
6.1.2.	Analys av engelsk språkförmåga.....	32
6.1.3.	Analys av frågeställningar.....	34
6.1.4.	Sammanställning av slutsatser .....	35
7.	Diskussion.....	37
7.1.	Metodval.....	37
7.2.	Resultatdiskussion .....	37
7.3.	Etiska aspekter .....	38
7.4.	Vetenskapliga aspekter .....	39
7.5.	Samhälleliga aspekter .....	39
7.6.	Framtida forskning .....	39
7.7.	Studiens begränsningar.....	40

Bilaga A - Webbenkät

# 1. Introduktion

Attacker som använder *social manipulation* är ett växande problem på Internet. Syftet med dessa attacker är att manipulera användare och företag till att ge ut känsliga uppgifter, såsom inloggningsuppgifter eller kreditkortsinformation. Social manipulation är en strategi som riktar sig direkt till människor och undviker i många fall de säkerhetsmekanismer som finns i ett nätverk eller system (Salahdine & Kaabouch, 2019). Syftet är att utnyttja *den mänskliga faktorn*, som enligt Diaz, Sherman och Joshi (2019) är ansvarig för 95% av alla säkerhetsincidenter på företag runtom i världen. Den mänskliga faktorn innefattar säkerhetsincidenter där anställda begått ett misstag eller blivit manipulerade av angripare. Salahdine och Kaabouch (2019) förklarar även att människor är den största sårbarheten i ett nätverk eftersom de har en benägenhet till att lita på andra människor.

En av de attacker som använder social manipulation är *phishing*, vilket är en av de vanligaste attackerna på Internet. Forskning har visat att människor i allmänhet har svårt att upptäcka phishing-mejl, till exempel visade Mihelic, Jevscek, Vrhovec och Bernik (2019) att 69,4% av deltagarna i deras studie klickade på ett phishing-mejl. En faktor till detta är att människor inte är medvetna om de säkerhetsindikationer som finns i mejlen. Dessutom finns det begränsningar och sårbarheter i de anti-phishing verktyg som skall hjälpa till att bekämpa phishing hotet. Forskning har även visat att människor, med tiden, ignorerar de varningar som verktygen utlöser (Kleitman, Law & Kay, 2018).

Phishing-attacker riktar sig direkt till människor och utmärker sig med sin tillämpning av social manipulation. Den största sårbarheten ligger därför i den mänskliga faktorn, vilket ger ett behov av att fokusera uppmärksamheten på hur människor hanterar phishing-mejl. Företag har därför börjat utbilda personal genom bland annat föreläsningar och phishing simulationer. Forskning visar dock att detta inte är tillräckligt för att minska hotet från phishing. Sheng, Holbrook, Kumaraguru, Cranor och Downs (2010) skriver i sin studie att 28% av deltagarna föll för phishing-mejl trots förberedelser genom bland annat utbildningshemsidor och anti-phishing spel. Furnell (2007) påpekar att människor oftast bortser från tekniska- och språkliga aspekter när de tolkar mejl. Istället fokuserar de på visuella faktorer som logotyper, teckensnitt eller dylikt. Därav är målet med denna studie att undersöka vilken inverkan språket har på svenska Internetanvändares mottaglighet för phishing. Detta skall ske genom att kartlägga skillnaden mellan hur bra svenska Internetanvändare är på att upptäcka phishing-mejl på svenska jämfört med engelska.

## 2. Bakgrund

Detta kapitel avser att ta upp nödvändig bakgrundsinformation kring phishing, dess olika begrepp och de problem som granskas i studien.

### 2.1. Vad är phishing

Idén med phishing är att angriparen skall lura sitt offer med ett lockbete för att sedan fiska upp personliga uppgifter. Därav tillkom ordet phishing som en variation av engelskans "fishing". Anti-Phishing Working Group (2019) använder definitionen: "*Phishing är ett IT-brott som använder både social manipulation och tekniska knep för att stjäla konsumenternas personliga- och finansiella uppgifter*". Enligt Chiew, Yong och Tan (2018) har dessa attacker existerat sedan 1995 och är idag en av de vanligaste attackerna på Internet.

Attacken sker oftast genom ett utskick av bluffmejl, där avsikten är att användaren skall klicka på en länk i mejlet. Länken leder vidare till en hemsida som utseendemässigt verkar vara legitim men som i själva verket är förfalskad. Användaren uppmanas sedan till att skriva personliga- eller ekonomiska uppgifter på den förfalskade hemsidan, vilket kan leda till förödande konsekvenser med avseende på ekonomisk förlust eller skadat rykte (Parsons, McCormac, Pattinson, Butavicius & Jerram, 2015).

### 2.2. Komponenter och metoder inom phishing

Chiew et al. (2018) skriver att en phishing-attack utgår från tre komponenter: ett *medium*, en *vektor* och en *metod*. Inom phishing nyttjas oftast Internet, SMS eller telefonsamtal som medium. Internet har flera associerade vektorer, till exempel e-post, sociala medier eller direkt meddelanden genom chattapplikationer. SMS och telefonsamtal har skapat sina egna vektorer inom phishing området: *smishing* och *vishing*. Dessa innebär att bedragaren erhåller offrets personliga- eller ekonomiska uppgifter genom att ta kontakt via SMS (smishing) eller telefonsamtal (vishing).

Två välkända och effektiva metoder inom phishing är *social manipulation* och *spear-phishing*. Social manipulation innebär att angriparen utnyttjar sitt offer genom att ingjuta en viss känsla, till exempel en rädsla att förlora något. Ett exempel på detta kan vara när en bedragare skickar ut bluffmejl som säger att vissa tjänster kan försvinna om offret inte klickar på länken i mejlet och följer beskrivningarna. Detta kan leda till att offret tar beslut som är baserade på känslor, vilket ökar effektiviteten av phishing-attacken (Chiew et al., 2018).

De senaste åren har spear-phishing populariserats som metodval vid utförande av phishing-attacker. Istället för ett massutskick av bluffmejl, så riktar sig dessa attacker till specifika individer, grupper eller organisationer. En spear-phishing attack innebär att bedragaren tar reda på personliga detaljer om offret, till exempel genom användning av sociala medier. Attacken utformas sedan med hjälp av den information som samlats in om offret, vilket kan innebära att bedragaren imiterar en person som offret känner och har förtroende för (Chiew et al., 2018).

### **2.3. Phishing – Ett växande problem**

Phishing är ett problem, inte bara för enskilda individer utan också för organisationer runtom i världen och kan resultera i förluster av mångmiljonbelopp. Federal Bureau of Investigation (2019) skriver i sin rapport att phishing var det IT-brott som utfördes mest under 2019. De estimerar den totala summan av ekonomiska förluster till cirka två miljarder dollar, där *VD-bedrägerier* stod för majoriteten av summan.

Det är inte bara ekonomin som kan påverkas vid en phishing-attack, även människors integritet är sårbar. Under 2018 genomfördes en phishing-attack mot företaget *Equifax*, där bedragarna låtsades vara representanter från stora banker och finansiella institut. Ett utskick av tusentals phishing-mejl resulterade i att bedragarna fick åtkomst till personliga uppgifter och kreditkortsinformation från 145 miljoner kunder (Salahdine & Kaabouch, 2019).

Sedan det första identifierade fallet av phishing 1995, har attackerna kontinuerligt ökat och blivit mer sofistikerade. Anti-Phishing Working Group (2016) skriver att det inträffade 1 609 phishing-attacker per månad under 2004, jämfört med 92 564 phishing-attacker per månad under 2016, vilket är en ökning på 5753%. Vidare skriver Anti-Phishing Working Group (2019) att 74% av de förfalskade hemsidorna som används i syfte för phishing även använder *HTTPS* (Hypertext Transfer Protocol Secure). *HTTPS* är ett protokoll som krypterar kommunikationen mellan användarens webbläsare och den besökta hemsidan. När en hemsida använder *HTTPS* så visas ett nyckellås bredvid adressfältet, vilket kan ge besökaren en indikation om att hemsidan är säker. Detta utnyttjas av bedragare för att få den förfalskade hemsidan att verka mer legitim och därmed öka attackens effektivitet.

En lyckad phishing-attack kan innebära stora skador för organisationer, exempelvis skadat rykte eller monetära förluster. Många organisationer har därför börjat använda phishing simulationer som ett medel till att öka medvetenheten och understödja behandlingen av

phishing hotet. En sådan simulation innebär att personalen får phishing-mejl skickade till sig, där organisationen sedan övervakar hur många som klickar på länken i mejlet. Dessa mejl är oftast formade på ett sätt som skall få personalen att svara snabbt, exempelvis genom att ingjuta en känsla av brådska (Williams, Hinds & Joinson, 2018). Trots phishing simulationer och utbildningar, skriver PhishMe (2016) i sin rapport att de anställda som redan svarat på simulerade phishing-mejl är 67% mer benägna till att svara på ett nytt phishing-mejl. Rapporten involverade åtta miljoner mejl som skickats till 3,5 miljoner anställda runtom i världen.

Gordon et al. (2019) har i sin studie utvärderat huruvida anställda på ett sjukhus kunde förbättra sin medvetenhet kring phishing genom 20 olika phishing simulationer. Totalt 5 416 anställda tog emot simulationerna, varav 740 av dessa fick gå ett träningsprogram i hantering av phishing då de tidigare i simulationen klickat på mer än fem mejl. Simulationerna resulterade i en gradvis minskning av antal anställda som klickade på mejlen, dock noterades ingen märkbar minskning för de som gick träningsprogrammet.

Det finns idag många olika tekniker för hur phishing skall hanteras, bland annat har utbildningar genom exempelvis online-spel visat sig vara effektiva. En studie visade att anti-phishing spelet *What.Hack* ökade deltagarnas förmåga att upptäcka phishing-mejl med 36,7% (Wen, Lin, Chen & Andersen, 2019). Det finns även mjukvarulösningar, bland annat autentiseringsmekanismer som validerar huruvida mejlet skickades från ett giltigt domännamn. Likaså finns det svartlistningstjänster, till exempel *Google Safe Browsing* som kan kontrollera en URL mot en lista av misstänkta hemsidor. Phishing är dock fortfarande ett ständigt hot då bedragarna är snabba på att hitta sårbarheter och kringgå de säkerhetsåtgärder som existerar (Gupta, Tewari, Jain & Agrawal, 2016).

## **2.4. Tidigare forskning**

Inom tidigare forskning saknas det information och data för det områdes som undersöks i denna studie. Den tidigare forskning som presenteras i detta delkapitel är dock fortfarande relevant för denna studie då det finns likheter inom utförandeprocessen. Dessutom kan resultat från tidigare forskning jämföras med resultatet från denna studie.

Hong, Kelley, Tembe, Murphy-Hill och Mayhorn (2013) utförde ett experiment där 53 deltagare medverkade i en webbenkät. Enkäten var rollspelsbaserad och deltagarna fick i uppdrag att ta sig an rollen som "Bob Jones". De skulle läsa igenom 14 mejl från "Bob Jones"

inkorg och kategorisera dessa som antingen phishing, skräppost, skadeprogram eller legitimt. Resultaten visade att 92% av deltagarna hade svårt att skilja på phishing- och legitima mejl.

Parsons et al. (2015) genomförde ett experiment med 117 deltagare som delades in i två grupper. Den första gruppen som kallades "Kontrollgruppen" fick information om att experimentet var en studie i hur de hanterade olika mejl, medan den andra gruppen hade blivit förvarnade om att de deltog i en studie om phishing. Gruppen som blivit förvarnade var bättre på att se skillnaden mellan ett legitimt mejl och ett phishing-mejl. En faktor till detta resultat var att gruppen blivit förvarnad om phishing studien, vilket bidrog till att de tog längre tid på sig. Resultatet visade också att 42% av alla mejl klassificerades felaktigt, vilket ger en antydning på människors bristande förmåga till att kategorisera mejl.

En studie utförd under 2018 på Universitetet i Maryland undersökte hur många av de 1 350 studenterna som var mottagliga för phishing-mejl. Studien bestod av tre phishing-mejl med olika implementationer av strategi. Det första mejlet efterliknade ett utskick från en bank och innehöll information om betalningsproblem. Det andra mejlet innehöll en belöning och informerade användare att de vunnit pengar i en tävling. Det tredje mejlet hotade användaren med att deras konto skulle upphävas inom ett visst datum. Resultatet visade att 60% av studenterna klickade på något av phishing-mejlerna, där 70% också öppnade länken i mejlet (Diaz et al., 2019).

Furnell (2007) bjöd in 179 personer till en webbenkät med totalt 20 mejl, där elva av dessa var phishing och nio legitima. Svarsalternativen som deltagarna fick använda var "*Legitim*", "*Illegitim*" och "*Vet inte*". För de legitima mejlerna hade deltagarna en felprocent på 37%, i jämförelse med de illegitima som hade 28,5%. Felprocenten med alla mejl kombinerade låg på 32%, varav 26% av deltagarna svarade "*Vet inte*". Studiens slutsats summerades med att människor inte vet vad de skall kolla efter i phishing-mejl. Förutom uppenbara ledtrådar som till exempel dålig stavning, påpekas det även att användaren skall göra en bedömning av phishing-mejlet baserat på vad det ber dem att göra. Ett exempel är att banker aldrig skickar ut mejl och ber om personliga uppgifter, lösenord eller inloggningskoder.

Williams et al. (2018) har i sin studie utvärderat huruvida strategier som involverar auktoritet och tidspress, har någon inverkan på phishing mottagligheten bland anställda. Ett phishing-mejl med auktoritetsstrategier fokuserar på att efterlikna organisationer eller individer som är respekterade och som har en viss makt över offret. Strategier som involverar tidspress

fokuserar på att mejlet skall innehålla någon form av stressmoment för att snabbt kunna få ett svar från offret.

Studien bestod av nio phishing-mejl som skickades till 62 000 anställda på ett företag. Alla mejl var formulerade med respektive individs namn för att göra det extra trovärdigt. Med en skala 1–3, betygsatte forskarna de nio mejlen utifrån den grad av auktoritet och tidspress de innehöll. Dessa två strategier bedömdes separat, vilket betyder att de kunde sammanräknas för att få ett totalt värde på mejlets svårighetsgrad. Studien pågick i sex veckor, därefter analyserades resultaten och baserades på personalens klick frekvens för varje mejl (Williams et al., 2018).

Mejlet med högst klick frekvens låg på 35%, där både auktoritet och tidspress fått betyget två, till ett totalt värde av fyra. Det mejl med näst högst klick frekvens låg på 34% och hade betyget tre för auktoritet samt 1,5 för tidspress, vilket ger ett totalt värde på 4,5. Det finns ett samband i studien där mejlen med hög klick frekvens också har ett högt totalt värde för auktoritet och tidspress. Fyra mejl med ett totalt värde på två (auktoritet ett och tidspress ett), hade en klick frekvens på mellan 6–10%. Ett mejl med ett totalt värde på två stod ut från mängden med en klick frekvens på 21%. Alla mejl tillsammans hade en genomsnittlig klick frekvens på cirka 20%, vilket betyder att var femte anställd öppnade ett phishing-mejl. Forskarna sammanfattar studien med antydning på att personal är mer benägna till att klicka på ett phishing-mejl om det involverar strategier som auktoritet och tidspress (Williams et al., 2018).

### 3. Problembakgrund

Detta kapitel behandlar och undersöker studiens problemområde. Dessutom presenteras de avgränsningar som gjorts, vilka resultat som förväntas och vad studien kan bidra med i framtiden.

#### 3.1. Problemområde

Syftet med studien är att undersöka skillnaden mellan svenska och engelska i förhållande till hur mottagliga svenska Internetanvändare är för phishing-mejl. Det huvudsakliga motivet med studien är att synliggöra ett relativt outforskat område som kräver mer uppmärksamhet. Bedragare kan utnyttja språket i ett phishing-mejl för att ge ett mer genuint intryck. Dessutom kan översättningsverktyg som till exempel *Google Translate* hjälpa bedragare att anpassa phishing-mejlen efter en användares modersmål. Språkkunskaper skiljer sig mellan individer, därav ingår det i motivet med studien att undersöka om detta påverkar mottagligheten för phishing hos svenska Internetanvändare. Språkkunskaper kan innebära att vissa individer ser lingvistiska fel i mejlet medan andra förbiser detta.

För att få svar på studiens syfte har tre frågeställningar formulerats:

1. *Hur bra är svenska Internetanvändare på att upptäcka phishing-mejl på svenska?*
2. *Hur bra är svenska Internetanvändare på att upptäcka phishing-mejl på engelska?*
3. *Hur stor är skillnaden mellan hur bra svenska Internetanvändare är på att upptäcka phishing-mejl på svenska jämfört med engelska?*

I dessa frågeställningar betraktades orden *bra* och *skillnaden* som alltför generella. Det är viktigt att tydliggöra vad dessa ord betyder då de skall beskriva ett mätbart värde. Eftersom de är generella ord kan de tolkas på olika sätt, till exempel kan ordet *bra* tolkas som hur snabbt deltagarna upptäcker phishing-mejlen. Därav definierades orden som följande:

- Bra: *Deltagarnas medelpoäng inom engelska- eller svenska phishing-mejl.*
- Skillnaden: *Skillnaden mellan deltagarnas medelpoäng inom engelska- och svenska phishing-mejl.*

### **3.2. Avgränsning**

Denna studie kommer att avgränsas till Internetanvändare i Sverige mellan åldrarna 18–81. Studien kommer inte att undersöka huruvida faktorer som ålder och kön påverkar hur väl deltagarna upptäcker phishing-mejl. Dessutom kommer studien inte att undersöka om vissa personlighetsdrag påverkar risken att falla för phishing. Likaså kommer studien inte att undersöka om vissa strategier i phishing-mejl påverkar risken att falla för phishing. Ovanstående avgränsningar gjordes då det redan finns studier som haft dessa faktorer i åtanke. Slutligen kommer studien inte att kontrollera deltagarnas utbildningsnivå, till exempel om de har en gymnasial- eller eftergymnasial utbildning. Istället kommer deltagarnas IT-kompetens att kontrolleras för att se om det påverkar hur väl de upptäcker phishing-mejl.

### **3.3. Mål och förväntat bidrag**

Området som studien avser att undersöka är relativt outforskat, vilket gör resultatet svårare att förutspå. De förväntade resultaten anges för varje frågeställning och baseras främst på tidigare forskning, tillsammans med egna antaganden.

*Hur bra är svenska Internetanvändare på att upptäcka phishing-mejl på svenska?*

Hypotesen är att deltagarna kommer kunna upptäcka de svenska phishing-mejlerna relativt effektivt. Då det svenska språket är deltagarnas modersmål, förväntas de kunna upptäcka lingvistiska fel i de svenska phishing-mejlerna. Dessutom är det sannolikt att de kan relatera till olika svenska företag och deras domänadresser.

*Hur bra är svenska Internetanvändare på att upptäcka phishing-mejl på engelska?*

Hypotesen är att deltagarna kommer ha svårt att upptäcka de engelska phishing-mejlerna. Engelska är deltagarnas andraspråk i denna studie, därav förväntas deltagarna ha en variation i sin engelska språkförmåga. Dessutom förväntas deltagarna ha mindre kännedom om utländska företag och deras domänadresser.

*Hur stor är skillnaden mellan hur bra svenska Internetanvändare är på att upptäcka phishing-mejl på svenska jämfört med engelska?*

Det förväntade resultatet är att deltagarna kommer vara bättre på att upptäcka phishing-mejl på svenska jämfört med engelska.

Förhoppningen är att studien skall ge upphov till ytterligare forskning inom detta specifika område. I kapitel 2.4 presenterades tidigare forskning som undersökt hur väl människor upptäcker engelska phishing-mejl. Eftersom det finns en avsaknad av data för andra språk än engelska kan denna studie bidra med att presentera data beträffande det svenska språket. Studien kan även bidra med att öka medvetenheten hos människor gällande det hot som phishing-attacker utgör. Likaså kan studien bidra med att visa hur viktig den språkliga delen är och att den kan användas till att upptäcka phishing-mejl. Förhoppningen är också att presentera data som kan vara av intresse för utvecklare av framtida säkerhetsverktyg. Utvecklarna kan då utifrån studiens resultat bedöma huruvida den språkliga delen kräver mer uppmärksamhet.

## 4. Metod

I detta kapitel presenteras studiens metod, population och urval, samt processen kring skapandet av enkäten. Kapitlet avslutas med reflektioner kring studiens validitet, etiska överväganden som gjorts och en sammanställning av studiens metod.

### 4.1. Processöversikt

Enkätundersökning är en process i flera delar. Innan enkäten skapas måste syftet med studien vara tydlig, dessutom bör diverse beslut göras kring avgränsningar, urval och etiska aspekter. En viktig del i processen är de frågor som enkäten grundar sig i och att dessa anpassas till studiens syfte. Enkäten kan distribueras till den valde populationen när alla väsentliga beslut har tagits och frågorna har formulerats i förhållande till studiens syfte. Distribuering sker vanligtvis genom utskick via post, Internet eller specifika fysiska miljöer. Då alla svar tagits emot skall en bortfallsanalys utföras, vilket kan medföra vissa kompensationer i studien. Detta kan till exempel innefatta deltagare som inte genomfört hela enkäten. När bortfallsanalysen är färdig kan analysarbetet påbörjas, vilket sedan skall leda till en komplett presentation av den data som tagits fram (Trost & Hultåker, 2016).

### 4.2. Forskningsmål

Denna studie utgår från en process som Trost och Hultåker (2016) beskriver i sin bok, där olika delmål skall uppnås innan nästa steg kan påbörjas. Denna process är indelad i fem steg: *förberedelser, skapandet av webbenkät, pilotstudie, datainsamling* samt *dataanalys*.

**Steg 1 - Förberedelser:** Det första steget går ut på att ta fram bakgrundsinformation om ämnet och samtidigt studera det för att förstå olika begrepp och problem. Detta innebär en fördjupning av relevant litteratur och en analys av vilken kunskap som redan finns inom ämnet.

**Steg 2 - Skapandet av webbenkät:** När förberedelserna genomförts skall webbenkäten skapas. Enkäten och frågorna bör noggrant anpassas för allmänheten så att de kan besvaras på ett sätt som ger reliabilitet samt validitet.

**Steg 3 – Pilotstudie:** Innan webbenkäten distribueras till allmänheten skall en pilotstudie utföras under en vecka. Denna nyttjas till att åtgärda eventuella fel och brister i enkäten innan den fullständiga distribueringen sker.

**Steg 4 – Datainsamling:** Webbenkäten skall distribueras till allmänheten under en treveckorsperiod. Detta ger tid till att kontinuerligt samla in den data som erhålls, samtidigt som det ger utrymme för allmänheten att besvara enkäten. Distribueringen sker genom sociala nätverk.

**Steg 5 – Dataanalys:** Den data som samlats in skall struktureras, analyseras och tolkas med hjälp av statistiska tekniker och verktyg.

### **4.3. Enkätmetodik**

Detta delkapitel presenterar hur enkäten togs fram och varför vissa val gjordes. Detta inkluderar diskussioner kring kvalitativa- och kvantitativa undersökningar, standardisering och strukturering i enkäten, formulering av enkätfrågorna samt val av population. Delkapitlet avslutas med de validitetshot som upptäcktes, diskussion kring etiska överväganden samt en sammanfattning av studiens metod.

#### **4.3.1. Kvalitativa och kvantitativa undersökningar**

Enligt Christoffersen och Johannessen (2015) är kvantitativa metoder mindre flexibla jämfört med kvalitativa. Frågorna i kvantitativa enkäter är oftast samma för alla deltagare och det finns ett visst antal svarsalternativ som redan är givna. En fördel med detta är att svaren kan jämföras utan att beakta olika perspektiv från samtliga deltagare. Däremot krävs noggrannhet gällande vilka frågor som skall vara med, hur de formuleras och vilka svar som passar bäst in. Trost och Hultåker (2016) skriver att en kvantitativ metod är bäst lämpad för studier där frågeställningarna innehåller formuleringar som *hur många*, *hur ofta* eller *hur vanligt*.

Inom kvalitativa metoder går det vara mer spontan och flexibel med deltagarna. Frågorna som ställs är öppna och kan anpassas beroende på individen. Deltagarna har inga fasta svar utan kan uttrycka sig fritt med egna ord, vilket ger mer detaljerade svar jämfört med kvantitativa undersökningar (Christoffersen & Johannessen, 2015).

Syftet med studien avgör huruvida en kvalitativ- eller kvantitativ metod skall användas. Denna studie använder en webbenkät vars syfte är att ta reda på hur stor skillnad det är mellan hur bra svenska Internetanvändare är på att upptäcka phishing-mejl på svenska jämfört med engelska. Deltagarna skall bedöma huruvida ett mejl är legitimt eller phishing, sedan omvandlas den insamlade datan till användbar statistik. En kvantitativ metod är därav relevant i detta syfte eftersom den insamlade datan är mätbar. Den kan därför användas till att presentera fakta och mönster som upptäckts i studien.

### 4.3.2. Standardisering & strukturering

*Standardisering* innebär att frågorna framställs på samma sätt för alla deltagare. Kvantitativa studier nyttjar oftast en högre grad av standardisering jämfört med kvalitativa studier. Enkäter med kvantitativ metod bör hålla en hög grad av standardisering då detta är optimala förhållanden vid jämförelser. *Strukturering* innebär hur väl utformad enkäten är med avseende på dess syfte. Enkäter med ett flertal frågor som inte hör till studiens syfte har en låg grad av struktur, medan det motsatta är sant för en hög grad av struktur (Troost & Hultåker, 2016).

Avsikten med denna studie är att ha en hög grad av både standardisering och strukturering. För att verkställa detta har medvetna val gjorts kring enkätens uppbyggnad, frågeformuleringar och svarsalternativ. Frågorna och svarsalternativen utvärderades av opartiska människor som inte är involverade i studien. Dessutom genomfördes en pilotstudie med avsikt att erhålla feedback kring eventuella brister och fel i enkäten.

### 4.3.3. Frågor och formuleringar

Det finns två typer av frågor i en enkät: *öppna* och *icke-öppna*. En fråga som är öppen har inga svarsalternativ, därav har deltagaren friheten att skriva ner ett eget svar. En icke-öppen fråga har ett specifikt antal fasta svarsalternativ som deltagaren kan välja bland (Troost & Hultåker, 2016). För denna studie fanns det inget syfte med öppna frågor, därav har endast icke-öppna frågor nyttjats i enkäten.

Det finns två problem gällande icke-öppna frågor i enkäter. Det första problemet är att svarsalternativen kan tolkas på olika sätt av deltagarna. Det är viktigt att se på svarsalternativen ur deltagarnas perspektiv för att göra enkäten mer begriplig. Det andra problemet med fasta svarsalternativ är att det oftast saknas detaljrikedom, vilket innebär att studien inte kan ge en omfattande bild kring resultaten (Troost & Hultåker, 2016). En fråga i studiens enkät som behandlade deltagarnas språkförmåga inom engelska var det största hotet mot dessa två problem. I denna fråga skulle deltagarna ange ett svarsalternativ som passade deras språkförmåga inom engelska. Detta var ett hot eftersom deltagarna har egna uppfattningar om sin engelska språkförmåga. Därav var det viktigt att ha en tydlig men kortfattad beskrivning av varje svarsalternativ. Council of Europe (2018) har skapat ramverket *CEFR* (Common European Framework of Reference for Languages), där de använder sex skalor som beskriver en människas språkförmåga. Denna studie har förkortat beskrivningen av skalorna i syfte att kunna använda dessa som svarsalternativ gällande frågan om deltagarnas språkförmåga inom engelska.

Generella frågor är ett vanligt problem i enkäter och innebär att hela frågan eller vissa ord är alltför övergripande. Det kan därför bli svårt för deltagarna att veta exakt vad som menas (Christoffersen & Johannessen, 2015). Under skapandet av studiens enkät har det funnits medvetenhet och åtanke kring detta problem. Dessutom utfördes en pilotstudie i syfte att kunna åtgärda eventuella brister i enkäten där bland annat frågeformulering ingick.

En annan detalj som bör kontrolleras inom enkäter är längden på frågeformuleringar och svarsalternativ. Det lämpligaste alternativet är att de går rakt på sak med en kort och specifik beskrivning. Långa frågor eller svarsalternativ tenderar att trötta ut deltagare eftersom de kan behöva gå tillbaka och läsa om för att förstå innebörden (Trost & Hultåker, 2016). Alla frågor i studiens enkät har kontrollerats tillsammans med andra människor som inte varit inblandade i arbetet, där avsikten var att förhindra ovanstående problem.

Enkätens omfattning är en subjektiv fråga som måste undersökas, till exempel genom en pilotstudie. Rent generellt så är kortfattade enkäter lämpligast och ger oftast en högre svarsprocent då de kräver mindre tid av deltagarna. Detta ger även en högre *reliabilitet* i studien, då det har ett samband med antal deltagare. Därav är det viktigt att analysera enkäten och ta bort onödiga frågor som kan påverka enkätens omfattning (Christoffersen & Johannessen, 2015). Studiens enkät innehöll 37 frågor, där fem av dessa var allmänna frågor om deltagaren medan de resterande 32 frågorna innefattade mejl som samlats in. Enkätens omfattning baserades på den feedback som erhöles från pilotstudien, där 37 frågor ansågs vara rimligt för en hög svarsprocent. Trost & Hultåker (2016) skriver att uppvärmningsfrågor är ett bra tillvägagångssätt för att stärka deltagarnas motivation och därmed öka svarsprocenten. I denna studie nyttjades därför två enkla frågor om deltagarnas kön och ålder som uppvärmningsfrågor.

#### **4.3.4. Population och urval**

Christoffersen och Johannessen (2015) beskriver populationen som den samling av människor som studien avser att undersöka. Populationen kan bli omfattande beroende på studiens målgrupp. I dessa fall kan en urvalsundersökning genomföras, där deltagare utses slumpmässigt och bildar ett representativt urval. Trost och Hultåker (2016) skriver att avsikten med den data som samlats in är att den skall kunna förespråka hela populationen. För att åstadkomma detta kan vissa strategier tillämpas vid urvalet. En av dessa strategier är ett obundet slumpmässigt urval, vilket innebär att studiens population nyttjas till att utse deltagarna slumpmässigt utan några speciella omständigheter. Först bör storleken av urvalet

bedömas utifrån en analys av populationen. Därefter kan ett verktyg nyttjas, till exempel en dator, för att slumpmässigt generera fram urvalsgruppen.

Ett stort urval ger en högre sannolikhet till att det är representativt för populationen, vilket bidrar till att studien genererar ett pålitligare resultat. Tidsaspekten är en faktor som bör beaktas vid beslut av urvalsstorleken. Ett större urval innebär att mer tid måste spenderas på att nå ut till alla deltagare och dessutom analysera fler svar. Det finns även ett samband mellan tid och kostnader, vilket innebär att utgifterna ökar i förhållande till den tid som nyttjas. Därmed infinner sig en balans mellan tillförlitligheten av studien och de resurser som finns till förfogande (Trost & Hultåker, 2016).

Studiens population avgränsades till Internetanvändare mellan åldrarna 18 – 81 med svenska som modersmål. Ett större urval ger en mer tillförlitlig studie, därför var målet att få så många deltagare som möjligt. För detta tillämpades ett slumpmässigt urval genom att distribuera enkäten via sociala medier. Syftet med detta var att utnyttja den sammankoppling av människor som finns på sociala medier och sprida enkäten till så många som möjligt.

#### **4.3.5. Verktyg vid genomförande**

SurveyMonkey (<https://www.surveymonkey.com>) valdes som verktyg för att skapa enkäten då det erbjöd alla relevanta funktioner. Under pilotstudien erhöles feedback från deltagarna som indikerade på att de ville ha möjligheten att se vilka mejl de svarat rätt och fel på. SurveyMonkey var kapabel till denna funktion och således implementerades detta i enkäten för alla mejlfrågor. En annan nyttig funktion var att all data kunde hanteras, analyseras och extraheras på ett smidigt sätt.

#### **4.3.6. Reliabilitet och validitet**

*Reliabilitet* innebär tillförlitligheten kring vilken data som använts, på vilket sätt den samlats in och hur den bearbetats (Christoffersen & Johannessen, 2015). Enkäten som nyttjades i studien hade en relativt simpel struktur där deltagarna fick ange huruvida ett mejl var äkta eller phishing. Mejlen fördelades i fyra grupper, med syftet att skilja på språken samt huruvida mejlen var legitima eller phishing. Dessa mejlgrupper matades sedan in som variabler i programvaran SPSS (IBM SPSS Statistics for Windows, Version 26.0). Därefter granskades svaren från alla deltagare, där en siffra mellan 0–8 matades in i SPSS under respektive mejlgrupp. Denna siffra baserades på antal rätt inom en specifik mejlgrupp. En viktig fråga i enkäten handlade om deltagarnas språkförmåga inom engelska, där deltagarna

kunde välja mellan sex skalor som baserades på *CEFRL*. Detta implementerades som en numerisk variabel i SPSS, där en siffra mellan ett och sex matades in baserat på deltagarens svar. Deltagarna fick även svara på om de hade någon utbildning eller jobb inom IT, varpå detta implementerades som en numerisk variabel i SPSS. I detta syfte nyttjades siffrorna noll och ett, där det förstnämnda innebar nej och det sistnämnda ja.

Validitet beskriver hur relevant data är i förhållande till verklighetens scenario. Studien skall mäta det den är avsedd till att göra, vilket innebär att frågorna bör vara utformade till att besvara studiens syfte (Christoffersen & Johannessen, 2015). Validitet inom forskningsvärlden brukar delas in i; *begreppsvaliditet*, *intern validitet*, *extern validitet* samt *validitet av statistiska slutsatser* (Wohlin et al., 2012).

*Begreppsvaliditet* innefattar till vilken grad studien mäter det den är avsedd till att göra. Om den data som samlats in är konkret och relevant i förhållande till studiens syfte, finns en hög grad av *begreppsvaliditet* (Christoffersen & Johannessen, 2015). Hot mot *begreppsvaliditet* innefattar forskarens förväntningar. I dessa fall kan forskaren medvetet eller omedvetet påverka resultatet i studien baserat på sina egna förväntningar. Ett annat hot är om studiens syfte, koncept eller frågor inte är tillräckligt definierade (Wohlin et al., 2012). En del i arbetet med denna studie var att samla in 32 mejl som skulle ligga på en liknande svårighetsgrad. Dessa mejl samlades in från privata mejllinkor samt diverse hemsidor på Internet. En del mejl visade länkar medan andra inte gjorde det, därav fattades beslutet att inte visa några länkar alls för att ge studien ett mer rättvist resultat.

*Intern validitet* beskriver huruvida det finns några omständigheter som utan forskarens kännedom kan påverka studiens resultat och slutsatser (Wohlin et al., 2012). Ett hot mot *intern validitet* som identifierats i denna studie är att enkätens omfattning kan skapa en känsla av tristess hos deltagarna. En pilotstudie utfördes med avsikt att ta del av deltagarnas feedback angående enkätens omfattning. Detta gav en uppfattning om hur enkätens storlek kunde justeras för att få en högre svarsprocent.

*Extern validitet* beskriver huruvida resultatet kan generaliseras till personer eller situationer utanför studiens omfattning. Ett av hoten mot *extern validitet* är om urvalet inte representerar de personer eller situationer som studien skall generaliseras till (Wohlin et al., 2012). För att minska detta hot, fattades beslutet att distribuera enkäten via sociala medier i syfte att nå en större och bredare population. I denna studie var det viktigt att urvalet representerade svenska

Internetanvändare i åldrarna 18 – 81 med svenska som modersmål. Därav var sociala medier en effektiv plattform för detta ändamål.

*Validitet av statistiska slutsatser* är ett mått på hur trovärdig studiens slutsats är. Ett hot mot detta är om studien har en låg statistisk effekt. Detta kan innebära att urvalsstorleken är för liten och den data som finns kan därför inte rättfärdiga studiens slutsats. Ett annat hot är om forskaren söker efter ett specifikt resultat, vilket kan bidra till att studien omedvetet konstrueras på ett sätt som skall uppfylla detta (Wohlin et al., 2012). En viktig aspekt för denna studie var att undvika en låg statistisk effekt med avseende på antal mejl i enkäten. Därav nyttjades 32 mejl i syfte att ha en balans mellan enkätens omfattning och låg statistisk effekt. Det infann sig en tidsbegränsning gällande studien, därav distribuerades enkäten under en treveckorsperiod med syftet att nå en så stor urvalsgrupp som möjligt.

#### **4.3.7. Etiska överväganden**

Forskningsetik kan avgränsas till etiska frågor kring de som medverkar i studien och forskareetik, det vill säga forskarens ansvar för sitt arbete. Forskare har inte bara ett ansvar för de individer som medverkar i studien, utan även för de som indirekt påverkas av forskningsresultatets betydelse. Forskareetik innebär att forskaren skall bedriva arbetet objektivt med en hög kvalitet, utan påverkan från omvärlden eller egna privata motiv (Vetenskapsrådet., 2017).

Ett ansvar som finns inom studier är hantering av deltagarnas personliga uppgifter. En riktlinje inom detta är att endast samla in den information som är nödvändig för att utföra forskningsarbetet. Denna information får endast nyttjas till att utföra det specifika ändamålet (ACM., 2018). Studiens enkät inkluderade en textruta där deltagarna frivilligt kunde skriva in sin e-postadress om de ville ta del av studiens fullständiga resultat. Enkäten innehåller inga krav där deltagare måste ange sina personuppgifter. Dessutom aktiverades en anonymitetsfunktion i SurveyMonkey som gör att deltagarnas IP-adress inte sparas.

I Vetenskapsrådet (2002) presenteras fyra krav på forskningsetik: *informationskravet*, *samtyckeskravet*, *konfidentialitetskravet* och *nyttjandekravet*. Dessa fyra agerar som riktlinjer i ett forskningsarbete och är väsentliga för att säkerställa ett sedligt korrekt arbete.

*Informationskravet* innebär att deltagarna skall informeras om studien syfte. *Samtyckeskravet* beskriver deltagarnas rätt till att bestämma över sin medverkan i studien.

*Konfidentialitetskravet* säkerställer att alla uppgifter i studien är konfidentiella och att

obehöriga inte kan få åtkomst till personliga uppgifter. *Nyttjandekravet* innebär att data endast får användas till det specifika forskningsarbetet.

Denna studie har använt de riktlinjer och krav som Vetenskapsrådet (2002) sammanställt.

Deltagarna presenteras först med information om studien och syftet med forskningen.

Därefter informeras deltagarna om att studien är helt anonym och att medverkandet är frivilligt. Avslutningsvis presenteras information om att data från enskilda individer inte kan urskiljas då svaren sammanställs i statistiska tabeller.

#### **4.4. Sammanställning av studiens metod**

En enkät med kvantitativ metod nyttjades som stöd till att besvara studiens syfte och frågeställningar. En viktig aspekt i studiens enkät var att den skulle ha en hög grad av standardisering och strukturering för att ge ett rättvist resultat. Därav konstruerades enkäten ur ett deltagarperspektiv med avseende på frågeformuleringar och ordval.

För att göra studien tillförlitlig och relevant, identifierades olika reliabilitet- och validitetshot.

Dessa innefattade låg statistiskeffekt, enkätens omfattning och låg standardisering.

Förhoppningen var att minska hotet för låg standardisering genom att göra enkäten enkel, tydlig och tillgänglig. Facebook ansågs vara en plattform som kunde distribuera enkäten, bidra till ett större urval och därmed minska hotet för låg statistisk effekt.

Olika etiska övervägningar gjordes i enkäten, där ändamålet var att följa informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet. Deltagarna fick ta del av studiens syfte, samt information om anonymitet och frivillig medverkan. Det fanns inget i studiens enkät som behandlade deltagarnas personliga- eller känsliga uppgifter.

Enkätverktyget SurveyMonkey användes till att skapa och distribuera enkäten via Facebook.

Tanken var att nå ut till många människor och samtidigt få en variation av åldrar och engelsk språkförmåga som kunde representera populationen. Studiens population avgränsades till Internetanvändare mellan åldrarna 18 – 81 med svenska som modersmål. En urvalsgrupp som kunde representera studiens population valdes sedan ut slumpmässigt genom Facebook.

En pilotstudie genomfördes under en veckas tid, i syfte att kunna åtgärda eventuella fel och brister i enkäten baserat på deltagarnas feedback. Under pilotstudien justerades enkäten genom att lägga till en frågesportsfunktion där deltagarna kunde se vilka mejl de svarat rätt och fel på.

Första sidan av enkäten innehåller information om studiens syfte, deltagarnas uppgift i enkäten samt en upplysning kring anonymitet och samtycke. Den andra sidan innehåller fyra allmänna frågor om deltagaren. Detta inkluderar kön och ålder, där dessa anses vara uppvärmningsfrågor som skall motivera individen till att fortsätta. Två av frågorna är relevanta för studien och involverar deltagarnas engelska språkförmåga samt IT-kompetens. Den tredje sidan innehåller 32 mejl där deltagarna skall svara huruvida de är legitima eller phishing. I bilaga A finns den enkät som nyttjades under studien.

#### **4.5. Dataanalys**

Den insamlade datan måste analyseras, varpå olika metoder används beroende på om datan är kvalitativ eller kvantitativ. Analysarbetet för kvalitativa data består av att bearbeta text, ljud, bild eller film medan kvantitativa data använder sig av olika statistiska tekniker för att utföra räkneoperationer (Christoffersen & Johannessen, 2015). Denna studie använder en kvantitativ metod, därav skall datan analyseras statistiskt.

Mejlen i enkäten delades in i fyra grupper baserat på typ och språk. Dessutom skapades grupper för engelsk språkförmåga och IT-kompetens. Dessa grupper nyttjades till att skapa sex variabler inom SPSS. Därefter granskades varje deltagare, varpå deras data extraherades till SPSS baserat på engelsk språkförmåga, IT-kompetens och antal rätt inom varje mejlgrupp.

Data från SurveyMonkey extraherades genom att filtrera frågorna baserat på dess mejlgrupp. Frågesportsfunktionen i enkäten visade sedan huruvida deltagaren svarat rätt eller fel på mejlfrågorna. Deltagarna fick ett poäng för varje rätt svar, där respektive mejlgrupp kunde ge som högst åtta poäng. Ett värde mellan 0–8 matades in i SPSS för varje mejlgrupp och deltagare.

Studiens dataanalys baserades på de fyra mejlgrupper som tagits ut från enkäten, samt grupperna för IT-kompetens och engelsk språkförmåga. Det första steget i dataanalysen var att kontrollera huruvida datan som samlats in var normalfördelad. Enligt Mendes och Pala (2003) är Shapiro-Wilks det test som är bäst lämpat när normalfördelning skall undersökas. Testet utfördes i SPSS och resultatet visade en signifikansnivå  $<0,05$  för varje mejlgrupp, vilket innebär att datan inte är normalfördelad. Dessutom nyttjades SPSS till att undersöka centralmått och diverse beskrivande statistik gällande mejlgrupperna. Därefter utformades hypoteser baserat på den framtagna statistiken.

Två olika hypotestester nyttjades för att prova de framtagna hypoteserna. McKnight och Najab (2010) skriver att *Mann-Whitney U* är ett icke-parametriskt test som lämpar sig bäst i de sammanhang där data inte är normalfördelad. Därav nyttjades Mann-Whitney U testet till att prova hypoteser gällande mejlgrupperna kombinerat med deltagarnas engelska språkförmåga och IT-kompetens. Rosner, Glynn och Lee (2005) skriver att *Wilcoxon Signed-Ranks* testet kan nyttjas i de sammanhang där datan inte är normalfördelad och när två variabler med samma population skall jämföras. Därav nyttjades Wilcoxon Signed-Ranks testet till att prova följande hypotes:

- H0: Det finns ingen skillnad mellan hur bra svenska Internetanvändare är på att upptäcka phishing-mejl på svenska jämfört med engelska.
- H1: Svenska Internetanvändare är bättre på att upptäcka phishing-mejl på svenska jämfört med engelska.

Vid hypotestestningarna nyttjades en signifikansnivå på 95%, vilket innebär att resultaten är signifikanta om  $p < 0,05$ .

## 5. Resultat

I detta kapitel presenteras resultaten från studien baserat på den insamlade datan från studiens webbenkät. Kapitlet börjar med en beskrivning av hur den insamlade datan strukturerades. Därefter presenteras övergripande statistik kring studiens urvalsgrupp, vilket innefattar antal deltagare samt kön- och åldersfördelning. Därefter presenteras resultaten från respektive mejlgrupp med koppling till IT-kompetens och engelsk språkförmåga. Alla frågor som nyttjats i studiens webbenkät kan ses i Bilaga A.

### 5.1. Strukturering av insamlade data

Det första steget i analysprocessen var att extrahera data från SurveyMonkey och strukturera den till variabler i SPSS. Relevanta variabler för studiens mål var engelsk språkförmåga, IT-kompetens samt fyra olika mejlgrupper baserade på mejlets typ och språk. Ett val som gjordes vid extrahering av data från SurveyMonkey var att använda ett filter för mejlgrupperna. Analysen av varje deltagare var därför en iterativ process med olika filter baserat på vilken mejlgrupp som skulle extraheras. Detta val gjordes i syfte att ha en organiserad process och för att undvika felinmatningar.

Den första gruppen innehöll data gällande deltagarnas engelska språkförmåga. För denna fråga fanns det sex svarsalternativ, därav skapades en variabel i SPSS med sex grupper. En siffra mellan 1–6 matades in under variabeln i SPSS beroende på vilket svarsalternativ som deltagaren valt i enkäten. Den andra gruppen baserades på frågan om deltagarnas IT-kompetens. Frågan innehöll två svarsalternativ vilket gjorde att variabeln i SPSS skapades med två grupper. Siffran noll matades in för de som svarat ”Nej” och siffran ett matades in för de som svarat ”Ja”.

De 32 mejl som nyttjats i enkäten fördelades i fyra grupper med åtta mejl vardera. Dessa grupper fördelades baserat på dess typ och språk. En frågesportsfunktion implementerades i enkäten med syfte att öka deltagarnas motivation och samtidigt förenkla analysarbetet. Frågesportsfunktionen gav deltagarna ett poäng för varje mejl som de kategoriserade korrekt. Fyra variabler för mejlgrupperna skapades i SPSS. En siffra mellan 0–8 matades in under varje mejlgrupp, där denna siffra baserades på den totala poängen som deltagaren fått under respektive mejlgrupp i enkäten.

Ett val som gjordes under analysarbetet var att dela in deltagarnas engelska språkförmåga i två grupper. Syftet med detta var att kunna jämföra två större grupper istället för sex mindre grupper. Dessutom fanns det en variation av antal deltagare mellan grupperna, vilket kunde ge ett skevt resultat. Deltagarnas engelska språkförmåga fördelades därför i följande grupper:

- Grupp 1: Innehåller 74 deltagare som valt *grundläggande, mellanliggande* eller *övre mellanliggande* som svarsalternativ.
- Grupp 2: Innehåller 78 deltagare som valt *avancerad* eller *behärskning* som svarsalternativ.

Denna fördelning möjliggjorde en jämförelse mellan två grupper, samtidigt som det finns en betydande skillnad mellan gruppernas engelska språkförmåga. En variabel med två grupper skapades i SPSS för detta avseende. Siffran ett eller två matades in under variabeln baserat på den grupp som deltagaren tillhörde. En översikt av struktureringen inom SPSS finns i Figur 1 nedan.

	RespondentID	SpråkID	IT_Komp	LSV	LEN	PSV	PEN	Split_Språk
1	1	3	1	5	3	7	8	1
2	2	2	0	8	4	7	7	1
3	3	6	1	7	7	7	6	2
4	4	5	0	5	3	6	6	2
5	5	5	0	6	4	6	4	2
6	6	2	0	5	5	7	6	1
7	7	5	0	7	7	7	5	2

**Figur 1.** Strukturen i SPSS tillsammans med en del av den insamlade datan.

## 5.2. Deltagare

Webbenkäten distribuerades via Facebook med avsikt att nå en bredare population. Enkäten hade totalt 218 deltagare med en slutförandefrekvens på 70%. Detta medförde att 66 deltagare försvann i bortfallsanalysen då de inte genomfört hela enkäten.

<b>Kön</b>	<b>Svarsprocent</b>	<b>Antal svar</b>
Män	51,32%	78
Kvinnor	48,68%	74
Annat	0%	0

**Tabell 1.** Könsfördelning och antal deltagare

Enkäten besvarades av 78 män och 74 kvinnor, vilket ger totalt 152 deltagare med användbara data. En övergripande bild av detta kan ses i Tabell 1.

## 5.3. Åldersfördelning bland deltagarna

Studiens urvalsgrupp bestod av svenska Internetanvändare mellan åldrarna 18–81. Enkäten besvarades till större delen av deltagare mellan åldrarna 18–49 med en total svarsprocent på 82,25%. Deltagare mellan åldrarna 50–81 utgjorde totalt 17,76% av svaren, där åldersgruppen 74–81 inte räknades med då inget svar kunde erhållas från denna grupp. En översikt av åldersfördelningen bland deltagarna kan ses i Tabell 2.

<b>Åldersgrupp</b>	<b>Svarsprocent</b>	<b>Antal svar</b>
18–25	19,74%	30
26–33	42,11%	64
34–41	13,82%	21
42–49	6,58%	10
50–57	5,92%	9
58–65	7,89%	12
66–73	3,95%	6
74–81	0%	0

**Tabell 2.** Åldersfördelning bland deltagarna.

## 5.4. Språkförmåga inom engelska

En fråga angående deltagarnas språkförmåga inom engelska skapades. Syftet med detta var att kunna undersöka om detta hade någon inverkan på hur bra deltagarna kategoriserade de engelska mejlen. Svartalternativen var baserade på skalor från CEFRL och förkortades enligt följande:

- Nybörjare - *Du kan presentera dig själv och använda mycket enkla ord och fraser.*
- Grundläggande - *Du kan förstå fraser och de vanligaste orden, samt kommunicera i enkla sammanhang.*
- Mellanliggande - *Du kan hantera de flesta situationer som kan uppstå under resor i ett område där engelska talas.*
- Övre Mellanliggande - *Du kan förstå huvudidéerna i komplex text och till en viss grad interagera flytande och spontant.*
- Avancerad - *Du kan läsa och förstå en stor mängd längre, krävande texter och använda engelska spontant, flexibelt och effektivt i sociala sammanhang.*
- Behärskning - *Du kan utan problem förstå allt som du hör eller läser och uttrycka dig helt flytande i så gott som alla situationer.*

Ingen av deltagarna beskrev sig som nybörjare på engelska, medan 48,7% ansåg sig ha en grundläggande, mellanliggande eller övre mellanliggande språkförmåga inom engelska. Avancerad var den skala som hade störst svarsprocent med 30,2%, medan behärskning var näst störst med 21,1%. När dessa två kombinerades utgjorde de 51,3% av deltagarna, vilket är mer än hälften av alla svar. I Tabell 3 visas fördelningen av deltagarnas engelska språkförmåga.

<b>Språkförmåga</b>	<b>Svarsprocent</b>	<b>Antal svar</b>
Nybörjare	0%	0
Grundläggande	12,50%	19
Mellanliggande	19,1%	29
Övre mellanliggande	17,1%	26
Avancerad	30,2%	46
Behärskning	21,1%	32

**Tabell 3.** Sammanfattning av deltagarnas språkförmåga.

## 5.5. IT-kompetens

En fråga angående deltagarnas IT-kompetens skapades i syfte att kunna undersöka huruvida det hade någon inverkan på hur bra deltagarna kategoriserade mejlen. Deltagarna fick besvara om de hade något jobb eller utbildning inom IT. Detta var en icke-öppen fråga med svarsalternativen ja eller nej.

Utbildning/Jobb inom IT	Svarsprocent	Antal svar
Ja	42,76%	65
Nej	57,24%	87

Tabell 4. Sammanfattning av deltagarnas IT-kompetens.

Enligt Tabell 4 så svarade 42,76% att de antingen hade ett jobb eller en utbildning inom IT, medan 57,24% svarade att de inte hade något av dessa.

## 5.6. Svenska legitima mejl

Gruppen för de svenska legitima mejlen matades in i SPSS som variabeln LSV. Beskrivande statistik sammanställdes för denna variabel kombinerat med grupperna för deltagare med eller utan IT-kompetens. Gruppen med IT-kompetens innehöll 65 deltagare och gruppen utan IT-kompetens innehöll 87 deltagare. Medelvärdet för antal rätt svar var marginellt högre för deltagare med IT-kompetens jämfört med de utan. Standardavvikelseerna tyder på att deltagarna inom gruppen med IT-kompetens hade en högre variation av antal rätt svar.

Variabel	Grupp	Medelvärde	Median	Standardavvikelse
LSV		5,49	6	1,933
LSV	IT-kompetens	5,66	6	2,131
LSV	Ingen IT-kompetens	5,36	6	1,772

Tabell 5. Beskrivande statistik gällande svenska legitima mejl.

Följande hypotes baserades på den beskrivande statistiken i Tabell 5 ovan:

- H0: IT-kompetensen bland svenska Internetanvändare har ingen betydelse när det gäller hur bra de är på att kategorisera svenska legitima mejl.
- H1: Svenska Internetanvändare med IT-kompetens är bättre på att kategorisera svenska legitima mejl jämfört med de utan IT-kompetens.

Ett Mann-Whitney U test nyttjades i syfte att prova denna hypotes. Ett p-värde  $<0,05$  innebär att resultatet är signifikant och  $H_0$  kan därför avfärdas i förmån för  $H_1$ .

Variabel	Grupp	Medelvärdesrang	Summa av rang	p
LSV	IT-kompetens	82,66	5373	0,130
LSV	Ingen IT-kompetens	71,9	6255	

**Tabell 6.** Resultat från Mann-Whitney U testet där  $p < 0,05$  innebär att resultatet är signifikant.

Data från Tabell 6 visar att  $p > 0,05$ , vilket innebär att resultatet inte är signifikant. Därmed kan  $H_0$  fastställas som en korrekt hypotes, vilket visar att IT-kompetensen bland svenska Internetanvändare inte har en betydelse när de skall kategorisera svenska legitima mejl.

### 5.7. Engelska legitima mejl

Gruppen för de engelska legitima mejlen matades in i SPSS som variabeln LEN. Beskrivande statistik gällande centralmått och standardavvikelse sammanställdes för variabeln. Dessutom kombinerades variabeln med grupper för deltagarnas IT-kompetens.

Variabel	Grupp	Medelvärde	Median	Standardavvikelse
LEN		4,12	4	2,079
LEN	IT-kompetens	4,74	5	2,153
LEN	Ingen IT-kompetens	3,67	3	1,909

**Tabell 7.** Beskrivande statistik gällande engelska legitima mejl.

Data från Tabell 7 visar att deltagare med IT-kompetens fick i genomsnitt 1,07 poäng mer när de kategoriserade de engelska legitima mejlen. Även medianvärdet visar att det finns en skillnad mellan de två grupperna, där deltagarna med IT-kompetens hade två poäng mer än deltagarna utan IT-kompetens. Värdena för standardavvikelse visar att det finns en marginell variation i antal rätt svar mellan grupperna.

Följande hypotes har tagits fram baserat på data från den beskrivande statistiken i Tabell 7 ovan:

- $H_0$ : IT-kompetensen bland svenska Internetanvändare har ingen betydelse när det gäller hur bra de är på att kategorisera engelska legitima mejl.
- $H_1$ : Svenska Internetanvändare med IT-kompetens är bättre på att kategorisera engelska legitima mejl jämfört med de utan IT-kompetens.

Ett Mann-Whitney U test nyttjades i syfte att prova denna hypotes. Ett p-värde  $<0,05$  innebär att resultatet är signifikant och  $H_0$  kan därför avfärdas i förmån för  $H_1$ .

Variabel	Grupp	Medelvärdesrang	Summa av rang	p
LEN	IT-kompetens	89,90	5843,50	0,001
LEN	Ingen IT-kompetens	66,49	5784,50	

**Tabell 8.** Resultat från Mann-Whitney U testet där  $p < 0,05$  innebär att resultatet är signifikant.

Data från Tabell 8 visar att  $p < 0,05$  vilket innebär att det finns en signifikant skillnad mellan grupperna för IT-kompetens. Därmed kan  $H_0$  avfärdas i favör för  $H_1$ . Detta visar att IT-kompetensen bland svenska Internetanvändare har en betydelse när de skall kategorisera engelska legitima mejl.

Gruppen för deltagarnas språkförmåga delades in i ytterligare två grupper. Ingen av deltagarna valde nybörjare som engelsk språkförmåga, därav uteslöts detta alternativ.

Fördelningen av grupperna blev på följande sätt:

- Grupp 1 innehöll 74 deltagare som valt grundläggande, mellanliggande eller övre mellanliggande som engelsk språkförmåga.
- Grupp 2 innehöll 78 deltagare som valt avancerad eller behärskning som engelsk språkförmåga.

Beskrivande statistik sammanställdes för de engelska legitima mejlen kombinerat med de två språkgrupperna.

Variabel	Grupp	Medelvärde	Median	Standardavvikelse
LEN	Grupp 1	3,49	3	1,988
LEN	Grupp 2	4,73	5	1,991

**Tabell 9.** Beskrivande statistik för engelska legitima mejl kombinerat med två språkgrupper.

Data från Tabell 9 visar att grupp 2 har ett medelvärde på 4,73, jämfört med grupp 1 som har 3,49. Detta innebär en skillnad på 1,24 poäng mellan grupperna. Även medianvärdena indikerar på att det finns en poängskillnad mellan grupperna. Värdena för standardavvikelse visar att det finns en variation för antal rätt svar inom grupperna, men ingen märkbar skillnad mellan grupperna.

Följande hypotes baserades på beskrivande statistik från Tabell 9 ovan:

- H0: Den engelska språkförmågan bland svenska Internetanvändare har inget inflytande på hur bra de kategoriserar engelska legitima mejl.
- H1: Svenska Internetanvändare med en avancerad eller behärskande engelsk språkförmåga är bättre på att kategorisera engelska legitima mejl, jämfört med de som har en grundläggande, mellanliggande eller övre mellanliggande engelsk språkförmåga.

Ett Mann-Whitney U test nyttjades i syfte att prova denna hypotes. Ett p-värde  $<0,05$  innebär att resultatet är signifikant och H0 kan därför avfärdas i förmån för H1.

Variabel	Grupp	Medelvärdesrang	Summa av rang	p
LEN	Grupp 1	62,16	4599,50	0,000
LEN	Grupp 2	90,11	7028,50	

**Tabell 10.** Resultat från Mann-Whitney U testet, där  $p < 0,05$  innebär att resultatet är signifikant.

Data från Tabell 10 visar att  $p < 0,05$ , vilket innebär att det finns en signifikant skillnad mellan grupperna för engelsk språkförmåga. Därmed kan H0 avfärdas i förmån för H1. Detta visar att den engelska språkförmågan bland svenska Internetanvändare har en betydelse när det handlar om hur bra de är på att kategorisera engelska legitima mejl.

## 5.8. Svenska phishing-mejl

Gruppen för de svenska phishing-mejlen matades in i SPSS som variabeln PSV. Beskrivande statistik sammanställdes för denna variabel och kombinerades med grupperna för IT-kompetens.

Variabel	Grupp	Medelvärde	Median	Standardavvikelse
PSV		6,61	7	0,862
PSV	IT-kompetens	6,74	7	0,815
PSV	Ingen IT-kompetens	6,52	7	0,887

**Tabell 11.** Beskrivande statistik för svenska phishing-mejl kombinerat med grupper för IT-kompetens.

Data från Tabell 11 visar en marginell skillnad på 0,22 poäng mellan gruppernas medelvärden. Medianvärdet visar ingen poängmässig skillnad mellan grupperna. Värdena för standardavvikelse tyder på att det finns en låg variation av antal rätt svar inom grupperna och en marginell skillnad mellan grupperna.

Följande hypotes baserades på data från den beskrivande statistiken i Tabell 11 ovan:

- H0: IT-kompetensen bland svenska Internetanvändare har ingen betydelse när det gäller hur bra de är på att kategorisera svenska phishing-mejl.
- H1: Svenska Internetanvändare med IT-kompetens är bättre på att kategorisera svenska phishing-mejl jämfört med de utan IT-kompetens.

Ett Mann-Whitney U test nyttjades i syfte att prova denna hypotes. Ett p-värde  $<0,05$  innebär att resultatet är signifikant och H0 kan därför avfärdas i förmån för H1.

Variabel	Grupp	Medelvärdesrang	Summa av rang	p
PSV	IT-kompetens	81,27	5282,50	0,203
PSV	Ingen IT-kompetens	72,94	6345,50	

**Tabell 12.** Resultat från Mann-Whitney U testet, där  $p < 0,05$  innebär att resultatet är signifikant.

Mann-Whitney U testet från Tabell 12 visar att  $p > 0,05$ , vilket innebär att resultatet inte är signifikant då det inte går att avfärda H0. Därför går det sammanfattningsvis säga att IT-kompetensen inte har någon betydelse när svenska Internetanvändare skall kategorisera svenska phishing-mejl.

## 5.9. Engelska phishing-mejl

Gruppen för de engelska phishing-mejlerna matades in i SPSS som variabeln PEN. Denna variabel kombinerades med grupper för IT-kompetens i syfte att sammanställa beskrivande statistik.

Variabel	Grupp	Medelvärde	Median	Standardavvikelse
PEN		6,41	7	1,171
PEN	IT-kompetens	6,49	7	1,062
PEN	Ingen IT-kompetens	6,36	7	1,248

**Tabell 13.** Beskrivande statistik för engelska phishing-mejl kombinerat med grupper för IT-kompetens.

Data från Tabell 13 visar en marginell skillnad på 0,13 poäng mellan gruppernas medelvärden, medan det inte finns någon skillnad på medianvärdena. Värden för standardavvikelse visar att det finns en låg variation av antal rätt svar inom grupperna.

Följande hypotes baserades på beskrivande statistik från Tabell 13 ovan:

- H0: IT-kompetensen bland svenska Internetanvändare har ingen betydelse när det gäller hur bra de är på att kategorisera engelska phishing-mejl.
- H1: Svenska Internetanvändare med IT-kompetens är bättre på att kategorisera engelska phishing-mejl jämfört med de utan IT-kompetens.

Ett Mann-Whitney U test nyttjades i syfte att prova denna hypotes. Ett p-värde  $<0,05$  innebär att resultatet är signifikant och H0 kan därför avfärdas i förmån för H1.

Variabel	Grupp	Medelvärdesrang	Summa av rang	p
PEN	IT-kompetens	78,68	5114	0,586
PEN	Ingen IT-kompetens	74,87	6514	

**Tabell 14.** Resultat från Mann-Whitney U testet, där  $p < 0,05$  innebär att resultatet är signifikant.

Mann-Whitney U testet från Tabell 14 visar att  $p > 0,05$ , vilket innebär att resultatet inte är signifikant då det inte går att avfärda H0. Därför går det sammanfattningsvis säga att IT-kompetensen inte har någon betydelse när svenska Internetanvändare skall kategorisera engelska phishing-mejl.

Beskrivande statistik sammanställdes gällande engelska phishing-mejl kombinerat med engelsk språkförmåga. För detta avseende nyttjades de grupper som tidigare skapats för de engelska legitima mejlen. Grupp 1 innehåller deltagare med grundläggande, mellanliggande och övre mellanliggande engelsk språkförmåga, medan grupp 2 innehåller deltagare med avancerad och behärskande engelsk språkförmåga.

Variabel	Grupp	Medelvärde	Median	Standardavvikelse
PEN	Grupp 1	6,46	7	1,173
PEN	Grupp 2	6,37	7	1,175

**Tabell 15.** Beskrivande statistik för engelska phishing-mejl kombinerat med två språkgrupper.

Data från Tabell 15 visar att det skiljer 0,09 poäng mellan gruppernas medelvärden. Det finns ingen skillnad i medianvärde mellan grupperna. Värden för standardavvikelse är nästan helt lika, vilket tyder på att variationen av antal rätt svar är likvärdig mellan grupperna.

Följande hypotes baserades på beskrivande statistik från Tabell 15 ovan:

- H0: Den engelska språkförmågan bland svenska Internetanvändare har inget inflytande på hur bra de kategoriserar engelska phishing-mejl.
- H1: Svenska Internetanvändare med en grundläggande, mellanliggande eller övre mellanliggande engelsk språkförmåga är bättre på att kategorisera engelska phishing-mejl jämfört med de som har en avancerad eller behärskande engelsk språkförmåga.

Ett Mann-Whitney U test nyttjades i syfte att prova denna hypotes. Ett p-värde  $<0,05$  innebär att resultatet är signifikant och H0 kan därför avfärdas i förmån för H1.

Variabel	Grupp	Medelvärdesrang	Summa av rang	p
PEN	Grupp 1	75,37	5749,50	0,736
PEN	Grupp 2	77,70	5878,50	

**Tabell 16.** Resultat från Mann-Whitney U testet, där  $p < 0,05$  innebär att resultatet är signifikant.

Data från Tabell 16 visar att  $p > 0,05$ , vilket innebär att det inte finns någon signifikant skillnad mellan grupperna för engelsk språkförmåga. Därmed fastställs H0 som en valid hypotes. Detta innebär att den engelska språkförmågan bland svenska Internetanvändare inte har något inflytande på hur bra de kategoriserar engelska phishing-mejl.

## **6. Analys och slutsats**

I detta kapitel presenteras analysprocessen för den insamlade datan, där syftet är att ge en detaljerad beskrivning över utformningen av denna process. Detta inkluderar en sammanställning och en analys av resultaten från kapitel 5. Avslutningsvis presenteras resultat med tillhörande analys för studiens hypotes och frågeställningar.

### **6.1. Analys av insamlade data**

Analysen av datan påbörjades efter att den strukturerats inom SPSS. Det huvudsakliga syftet med datan var att besvara studiens frågeställningar. Utöver detta fanns det även intresse till att undersöka andra aspekter. Upplägget med studiens resultat blev därför att först undersöka datan ur olika synvinklar gällande deltagarnas IT-kompetens och engelska språkförmåga. Därefter var avsikten att besvara studiens hypotes och frågeställningar med den data som samlats in.

#### **6.1.1. Analys av IT-kompetens**

Diaz et al. (2019) genomförde tre experiment där de skickade phishing-mejl till studenter inom olika högskoleprogram. Resultatet visade att studenter med IT-relaterade utbildningar var minst mottagliga för phishing-mejl. Kleitman et al. (2018) påpekar dock att det inte går att hitta något konsekvent samband mellan IT-kompetens och phishing mottaglighet.

Anledningen till detta är att det finns en tydlig skillnad i hur studierna mäter deltagarnas IT-kompetens.

Det förväntade resultatet i denna studie var att deltagare med IT-kompetens skulle vara bättre på att kategorisera mejlen jämfört med de utan IT-kompetens. Detta baserades på forskning från Diaz et al. (2019), samt egna antaganden om att de med IT-kompetens har tillbringat mer tid vid en dator och bör därav ha mer kännedom kring olika hot.

Relevant statistik som medelvärde, median och standardavvikelse sammanställdes, där avsikten var att skapa hypoteser baserat på statistiken. Därefter utfördes Shapiro-Wilks test på de relevanta variablerna inom SPSS för att undersöka normalfördelningen. Resultatet visade att det inte fanns någon normalfördelning för någon av mejlgrupperna när de kombinerades med IT-kompetens. Därav valdes Mann-Whitney U som test till att prova de hypoteser som tagits fram. En sammanfattning av alla mejlgrupper kombinerat med IT-kompetens kan ses i Tabell 17 nedan.

Variabel	Grupp	Medelvärde	Median	Standardavvikelse	p
LSV	IT-kompetens	5,66	6	2,131	0,130
	Ingen IT-kompetens	5,36	6	1,772	
LEN	IT-kompetens	4,74	5	2,153	0,001
	Ingen IT-kompetens	3,67	3	1,909	
PSV	IT-kompetens	6,74	7	0,815	0,203
	Ingen IT-kompetens	6,52	7	0,887	
PEN	IT-kompetens	6,49	7	1,062	0,586
	Ingen IT-kompetens	6,36	7	1,248	

**Tabell 17.** Sammanställning av IT-kompetens kombinerat med alla mejlgrupper.

Enligt Tabell 17 så har deltagare med IT-kompetens ett högre medelvärde i alla mejlgrupper. Inom gruppen med engelska legitima mejl finns det en betydande skillnad i medelvärde (1,07 poäng) tillsammans med ett signifikant resultat ( $p = 0,001$ ). Resultatet visar starka indikationer på att IT-kompetensen bland svenska Internetanvändare är en viktig faktor vid kategorisering av engelska legitima mejl. Det finns marginella skillnader i medelvärdena för svenska legitima mejl (0,3 poäng), svenska phishing-mejl (0,22 poäng) och engelska phishing-mejl (0,13 poäng). Detta tyder på att IT-kompetensen bland svenska Internetanvändare inte har någon betydande faktor vid kategorisering av dessa mejlgrupper.

### 6.1.2. Analys av engelsk språkförmåga

Kleitman et al. (2018) visade i sin studie att den engelska språkförmågan hos deltagarna hade en positiv effekt på hur de kategoriserade engelska legitima mejl. De med engelska som förstaspråk var bättre på att kategorisera de legitima mejlen, jämfört med de utan engelska som förstaspråk.

I denna studie fick deltagarna välja mellan sex svarsalternativ som var baserade på CEFRL-skalan. Det svarsalternativ de valde, beskrev deras engelska språkförmåga. Svarsalternativen fördelades i två grupper:

- Grupp 1: Grundläggande, mellanliggande och övre mellanliggande.
- Grupp 2: Avancerad och behärskning.

Denna studie innehåller deltagare med svenska som modersmål, därför går det inte dra en direkt koppling till studien av Kleitman et al. (2018). Däremot finns det indikationer på en koppling mellan människors språkförmåga inom ett språk och hur bra de är på att kategorisera mejl inom det språket. Det förväntade resultatet var därför att deltagare i grupp 2 skulle vara bättre än grupp 1 på att kategorisera de engelska mejlen.

Beskrivande statistik sammanställdes för grupperna med engelsk språkförmåga kombinerat med mejlgrupperna. Därefter skapades hypoteser baserat på denna statistik. Ett Shapiro-Wilks test utfördes på relevanta variabler i syfte att testa normalitet i datan. Resultatet visade att det inte fanns någon normalfördelning, därav nyttjades Mann-Whitney U testet till att prova hypoteserna. I Tabell 18 nedan finns en sammanställning av mejlgrupperna kombinerat med grupperna för deltagarnas engelska språkförmåga.

Variabel	Grupp	Medelvärde	Median	Standardavvikelse	p
LEN	Grupp 1	3,49	3	1,988	0,000
	Grupp 2	4,73	5	1,991	
PEN	Grupp 1	6,46	7	1,173	0,736
	Grupp 2	6,37	7	1,175	
LSV	Grupp 1	5,32	5,5	1,681	0,080
	Grupp 2	5,64	6	2,144	
PSV	Grupp 1	6,54	7	0,968	0,668
	Grupp 2	6,68	7	0,747	

**Tabell 18.** Mejlgrupper kombinerat med grupper för engelsk språkförmåga.

Enligt Tabell 18 så har grupp 2 ett högre medel- och medianvärde för de engelska legitima mejlen. Det skiljer 1,24 poäng mellan gruppernas medelvärden och två poäng mellan gruppernas medianvärden, där hypotestestet visar att denna skillnad är signifikant ( $p = 0,000$ ). Poängskillnaden tillsammans med p-värdet ger därför starka indikationer på att deltagarnas engelska språkförmåga påverkar hur bra de kategoriserar engelska legitima mejl. Detta är likt det resultat som Kleitman et al. (2018) fick i sin studie, där den engelska språkförmågan hade en inverkan på hur bra deltagarna kategoriserade engelska legitima mejl. Det finns marginella skillnader mellan grupperna inom engelska phishing-mejl (0,09 poäng,  $p = 0,736$ ), svenska legitima mejl (0,32 poäng,  $p = 0,080$ ) och svenska phishing-mejl (0,14 poäng,  $p = 0,668$ ). Detta tyder starkt på att deltagarnas engelska språkförmåga inte påverkar hur bra de kategoriserar dessa mejlgrupper.

Det finns en betydande skillnad mellan grupperna för de engelska legitima mejlen, medan det endast finns en marginell skillnad mellan grupperna för de engelska phishing-mejlen. Detta kan tyda på att deltagarna använder icke-språkliga ledtrådar till att identifiera de engelska phishing-mejlen. Den marginella skillnaden för de svenska mejlen kan förklaras med att alla deltagare ligger på en liknande språkförmåga inom svenska då det är deras modersmål.

### 6.1.3. Analys av frågeställningar

Dessa tre frågeställningar skapades med avsikt att besvara studiens syfte:

1. *Hur bra är svenska Internetanvändare på att upptäcka phishing-mejl på svenska?*
2. *Hur bra är svenska Internetanvändare på att upptäcka phishing-mejl på engelska?*
3. *Hur stor är skillnaden mellan hur bra svenska Internetanvändare är på att upptäcka phishing-mejl på svenska jämfört med engelska?*

Syftet med de två första frågeställningarna var att de skulle agera som underlag till den tredje frågeställningen. Detta underlag nyttjades sedan till att skapa en hypotes för den tredje frågeställningen.

Data för de två första frågeställningarna fanns tillgängligt i Tabell 11 och Tabell 13. Denna data sammanställdes i Tabell 19 nedan för att ge en tydligare överblick av resultatet.

Variabel	Medelvärde	Median	Standardavvikelse
PSV	6,61	7	0,862
PEN	6,41	7	1,171

**Tabell 19.** Sammanställning av beskrivande statistik för phishing-mejlgrupperna.

Enligt beskrivande statistik från Tabell 19 hade svenska Internetanvändare ett medelvärde på 6,61 poäng och ett medianvärde på sju poäng gällande svenska phishing-mejl. För de engelska phishing-mejlerna hade deltagarna ett medelvärde på 6,41 poäng och ett medianvärde på 7 poäng. Detta innebär en skillnad på 0,2 poäng mellan medelvärdena för svenska- och engelska phishing-mejl. Däremot upptäcktes ingen skillnad i medianvärdet mellan de två grupperna. Värden för standardavvikelser indikerar på att det finns en variation i antal rätt svar mellan grupperna.

I en studie av Furnell (2007) skulle deltagarna kategorisera mejl som antingen legitima eller phishing. Resultatet visade att deltagarna hade en felprocent på 28,5% när de kategoriserade phishing-mejlerna. Det förväntade resultatet för den första frågeställningen var att de svenska Internetanvändarna skulle upptäcka svenska phishing-mejl på ett relativt effektivt sätt. I denna studie hade deltagarna en genomsnittlig felprocent på 17,4% för de svenska phishing-mejlerna. Det förväntade resultatet för den andra frågeställningen var att de skulle ha svårt med att upptäcka phishing-mejl på engelska. I denna studie hade deltagarna en genomsnittlig felprocent på 20% för de engelska phishing-mejlerna. Båda dessa resultat anses vara bra i

förhållande till de resultat som Furnell (2007) presenterat i sin studie. Ett antagande var dock att det skulle finnas en större skillnad mellan svenska och engelska phishing-mejl.

Data från Tabell 19 ovan presenterade ett svar på de två första frågeställningarna, vilket gav upphov till följande hypotes angående den tredje frågeställningen:

- H0: Det finns ingen skillnad mellan hur bra svenska Internetanvändare är på att upptäcka phishing-mejl på svenska jämfört med engelska.
- H1: Svenska Internetanvändare är bättre på att upptäcka phishing-mejl på svenska jämfört med engelska.

Ett Shapiro-Wilks test utfördes på relevanta variabler i syfte att testa normalitet i datan. Resultatet visade att det inte fanns någon normalfördelning, därav nyttjades ett Wilcoxon Signed-Ranks test i syfte att prova ovanstående hypotes. Detta test används till att jämföra skillnaden mellan två variabler med samma population. Ett antagande gällande detta test är att det inte finns någon normalitet i datan (Rosner et al., 2005). Ett p-värde  $<0,05$  innebär att resultatet är signifikant och H0 kan därför avfärdas i förmån för H1.

Variabler	Medelvärde	Median	Standardavvikelse	p
PSV	6,61	7	0,862	0,039
PEN	6,41	7	1,171	

**Tabell 20.** Resultat från Wilcoxon Signed-Ranks testet där  $p < 0,05$  innebär att resultat är signifikant.

Data från Tabell 20 visar att p-värdet  $<0,05$ , vilket innebär att det finns en signifikant skillnad mellan mejlgrupperna och att H0 kan avfärdas i förmån för H1. Det finns dock en marginell skillnad mellan gruppernas medelvärden (0,2 poäng), samtidigt som det inte finns någon skillnad mellan deras medianvärden. Baserat på p-värdet och den marginella poängskillnaden finns det svaga indikationer på att svenska Internetanvändare är bättre på att upptäcka phishing på svenska jämfört med engelska.

#### 6.1.4. Sammanställning av slutsatser

Det finns en signifikant skillnad ( $p = 0,039$ ) mellan hur väl svenska Internetanvändare upptäcker phishing på svenska jämfört med engelska. Deltagarnas medelpoäng var 6,61 för de svenska phishing-mejlen och 6,41 för de engelska phishing-mejlen. Detta ger en marginell poängskillnad på 0,2 poäng mellan mejlgruppernas medelpoäng. Deltagarna hade en felprocent på 20% för de engelska phishing-mejlen och 17 % för de svenska phishing-mejlen, vilket ger en marginell skillnad på 3%. Resultatet visar därmed svaga indikationer på att

svenska Internetanvändare är bättre på att upptäcka phishing på svenska jämfört med engelska.

Deltagarna i studien delades in i två grupper baserat på deras engelska språkförmåga. Den första gruppen innehöll deltagare med grundläggande, mellanliggande och övre mellanliggande språkförmåga. Den andra gruppen innehöll deltagare med avancerad eller behärskande engelsk språkförmåga. Resultatet visade en signifikant skillnad ( $p = 0,000$ ) mellan grupperna när de skulle identifiera engelska legitima mejl. Skillnaden mellan gruppernas medelpoäng var 1,24, där den första gruppen hade 3,49 medan den andra gruppen hade 4,73. Resultatet visar starka indikationer på att engelsk språkförmåga är en betydande faktor vid identifiering av engelska legitima mejl.

Deltagarna delades även in i två grupper baserat på huruvida de hade någon utbildning eller jobb inom IT. Resultatet visade en signifikant skillnad ( $p = 0,001$ ) mellan grupperna när de skulle identifiera engelska legitima mejl. Skillnaden mellan gruppernas medelpoäng var 1,07, där deltagare med hög IT-kompetens hade 4,74 medan deltagare med lägre IT-kompetens hade 3,67. Resultatet visar starka indikationer på att IT-kompetens är en betydande faktor vid identifiering av engelska legitima mejl.

Det finns en marginell skillnad mellan grupperna för engelsk språkförmåga vid identifiering av phishing- och legitima mejl på svenska. Detta resultat är förväntat eftersom deltagarnas modersmål är svenska. Däremot är det förvånande att det inte finns någon betydande skillnad mellan grupperna vid identifiering av engelska phishing-mejl. Resultatet tyder därför på att deltagarna kan ha nyttjat icke-språkliga ledtrådar till att identifiera de engelska phishing-mejlen.

## **7. Diskussion**

Detta kapitel innehåller diskussioner och tankar kring studiens metod och resultat. Dessutom diskuteras diverse etiska, vetenskapliga- och samhällsliga aspekter kring arbetet. Kapitlet avslutas med förslag på framtida forskning i anknytning till studiens område.

### **7.1. Metodval**

Frågeställningarna utgjorde grunden för vilken metod som arbetet skulle använda. Metodvalet baserades därför på det tillvägagångssätt som var mest optimalt till att besvara frågeställningarna. Denna studie krävde inga detaljerade svar eller öppna diskussioner som litteraturstudier eller intervjuer kan tillhandahålla. Det var därför tydligt att enkätmetodik var det mest passande alternativet för studiens ändamål.

Enkätmetoden var, i kombination med sociala medier, ett effektivt sätt att nå ut till en större population, samtidigt som användbara svar kunde erhållas. Eftersom många människor i dagens samhälle använder smarttelefoner istället för datorer, fanns det en viss oro över huruvida mejlen i enkäten skulle synas ordentligt i telefonerna. Detta visade sig inte vara något problem baserat på responsen från pilotstudien och den huvudsakliga enkäten.

### **7.2. Resultatdiskussion**

Ett noterbart resultat från studien är den poängmässiga skillnaden mellan phishing- och legitima mejl. De svenska legitima mejlen har ett medelvärde på 5,49 poäng, medan de svenska phishing-mejlen har ett medelvärde på 6,61 poäng. De engelska legitima mejlen har ett medelvärde på 4,12 poäng, medan de engelska phishing-mejlen har ett medelvärde på 6,41 poäng. Detta ger en skillnad på 1,12 poäng för de svenska mejlen och 2,29 poäng för de engelska mejlen. Detta innebär att de legitima mejlen var svårare att kategorisera jämfört med phishing-mejlen. En förklaring till detta kan vara att phishing-mejl är lättare att upptäcka då de oftast innehåller någon ledtråd som kan avslöja mejlet. Dessutom kan det ha funnits en psykologisk aspekt gällande studiens syfte och dess relation till phishing-mejl. Därav fanns det potential till att deltagarna valde phishing som svarsalternativ på mejl som de var osäkra på.

Enligt studiens resultat är deltagare med IT-kompetens bättre på att kategorisera mejl jämfört med de utan IT-kompetens. Detta kan jämföras med studien som Diaz et al. (2019) utförde, där de kom fram till att deltagare med IT-relaterade utbildningar var mindre mottagliga för

phishing-mejl. Resultatet från denna studie var inte oväntat och det kan finnas olika faktorer som förklarar resultatet. Människor med IT-kompetens har oftast en ökad kunskap och medvetenhet kring säkerhetsaspekter som är relaterade till IT. Detta kan bidra till att de är extra försiktiga när de granskar mejlets struktur och diverse ledtrådar.

Det resultat som studien presenterat visar att deltagarnas engelska språkförmåga är en relevant indikator för hur bra de är på att kategorisera phishing- och legitima mejl på engelska. Det fanns en signifikant betydelse för den engelska språkförmågan, i förhållande till hur bra deltagarna var på att kategorisera engelska legitima mejl. Däremot fanns det ingen signifikant betydelse gällande de engelska phishing-mejlen. En möjlig förklaring till detta är att deltagarna kunde urskilja phishing-mejlen baserat på till exempel sändarens e-postadress. Alla legitima mejl har giltiga e-postadresser, vilket gör att deltagaren måste använda texten i mejlet som ledtråd. Deltagarna måste därför använda sina engelska språkförmågor genom att läsa igenom texten i mejlet och därefter utvärdera huruvida det var legitimt eller phishing. Detta ger en tydligare indikation på om skillnaden mellan deltagarnas engelska språkförmågor har någon betydelse.

Resultatet visar även att svenska Internetanvändare är bättre på att upptäcka phishing-mejl på svenska jämfört med engelska. Detta resultat var förväntat eftersom deltagarnas modersmål var svenska. Dessutom finns det ett antagande att majoriteten av deltagarna har mer kännedom om mejl från svenska företag jämfört med engelska. Det är också troligt att deltagarna var bättre på att se lingvistiska fel i de svenska mejlen jämfört med de engelska. Det är även viktigt att notera mejlens svårighetsgrad och hur detta kan påverka resultatet. Det finns en möjlighet att de engelska mejlen, bortsett från språket, var svårare att upptäcka rent generellt.

### **7.3. Etiska aspekter**

Totalt 152 individer svarade på studiens webbenkät, därav fanns det ett ansvar gentemot olika etiska principer. Detta involverade bland annat behandling av deltagarnas personliga uppgifter och anonymitet, men även objektiviteten kring studiens utförande och resultat. Det fanns inget inom enkäten som krävde att deltagarna skulle uppge några personliga- eller känsliga uppgifter. Däremot var det frivilligt för deltagarna att mata in en e-postadress om de ville ta del av studiens resultat och slutsats. Dessa sparades konfidentiellt fram till studiens slutförande. Dessa e-postadresser raderades efter att studiens resultat och slutsats skickats ut till deltagarna.

#### **7.4. Vetenskapliga aspekter**

Ingen av den tidigare forskning som granskats i kapitel 2.4 har jämfört modersmålet hos en population med deras andraspråk. En del studier tar upp språket som en viktig faktor när phishing-mejl skall upptäckas. Det finns dock inga studier som endast fokuserar på språkets inverkan på människors mottaglighet för phishing. Denna studie kan bidra till att skapa ett intresse för ett forskningsområde inom phishing, där avsikten är att belysa språkets inverkan på människors mottaglighet för phishing.

#### **7.5. Samhälleliga aspekter**

Språket är en betydande faktor när ett mejl skall kategoriseras som antingen legitimt eller phishing. En bedragare kan få mejlen att verka mer legitima genom att gömma ledtrådar, till exempel sändarens e-postadress, mejlets logotyp och länkadresser. Även texten i mejlet kan anpassas efter en specifik individ i syfte att verka mer legitim. En människas språkförmåga inom det språk som mejlet nyttjar, kan då ha en stor inverkan på huruvida de upptäcker phishing-mejlet eller inte.

Resultat i denna studie visade att svenska Internetanvändare är bättre på att upptäcka phishing-mejl på svenska jämfört med engelska. Studien bidrar med ökad kännedom kring språkets betydelse när det handlar om att upptäcka phishing-mejl. En förhoppning är att det även ger upphov till fortsatt forskning kring ämnet. Detta kan i sin tur medföra en ökad utveckling av anti-phishing verktyg, som kan hjälpa användare att avgöra huruvida ett mejl är legitimt eller phishing baserat på språket.

#### **7.6. Framtida forskning**

Det vore intressant att se om andra studier genererar ett liknande resultat som denna. Dessa studier kan då använda ett annat modersmål än svenska. Detta kan ge ytterligare indikationer på att människor i allmänhet är bättre på att upptäcka phishing-mejl på sitt modersmål jämfört med deras andraspråk.

Parsons et al. (2015) utförde en phishing studie, där syftet var att undersöka hur bra deltagarna var på att upptäcka phishing-mejl. I studien medverkade 117 deltagare som fördelades i två grupper. Den ena gruppen blev informerade om studiens syfte, medan den andra gruppen inte blev informerade. Resultatet visade att gruppen som blivit informerade om studiens syfte var bättre på att upptäcka phishing-mejl.

I denna studie fick alla deltagare reda på att de medverkade i en studie om phishing. Framtida forskning skulle kunna lägga till en aspekt, där deltagarna inte vet att de medverkar i en studie som handlar om phishing. Detta kan hjälpa till att skapa ett mer verklighetsbaserat scenario.

### **7.7. Studiens begränsningar**

Deltagarna visste om studiens syfte innan genomförandet av enkäten, vilket anses vara en begränsning i förhållande till studiens resultat. I ett verklighetsbaserat scenario skulle deltagarna inte få några förvarningar om att mejlet kunde vara phishing. Därav finns det begränsningar i studiens utförande, vilket kan påverka resultatens tillämpningar utanför studiens omfattning. En begränsning gällande standardisering i studien, upptäcktes i frågan *"Har du någon utbildning/jobb inom IT?"*. Utbildning kunde till exempel tolkas som gymnasial- eller eftergymnasialutbildning, medan jobb kunde tolkas som allt mellan nyttjandet av en dator, till underhåll och drift av servrar. Därav fanns det potential till att deltagarna svarade "Ja", även om de inte hade någon IT-kompetens enligt frågans egentliga mening.

En annan väsentlig del som kunde påverka studiens resultat, var de mejl som nyttjades i enkäten. Alla mejl samlades in med ändamålet att de skulle ha en liknande svårighetsgrad. Anledning till detta var att objektiviteten kring studiens resultat skulle öka om alla mejl låg på en liknande svårighetsgrad. På grund utav tidsbrist, kunde detta dock inte genomföras på ett systematiskt tillvägagångssätt. Därav fanns det potential till en växlande svårighetsgrad mellan mejlen, vilket kunde påverka studiens slutresultat.

## Referenser

- ACM. (2018). *ACM Code of Ethics and Professional Conduct*. Hämtad 2020-03-25, från <https://www.acm.org/code-of-ethics>
- Anti-Phishing Working Group. (2016). *Phishing Activity Trends Report: 4th Quarter 2016*. [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q4\\_2016.pdf](https://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf)
- Anti-Phishing Working Group. (2019). *Phishing Activity Trends Report: 4th Quarter 2019*. [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q4\\_2019.pdf](https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf)
- Chiew, K., Yong, K., & Tan, C. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems With Applications*, 106, 1-20. doi: 10.1016/j.eswa.2018.03.050
- Christoffersen, L. & Johannessen, A., 2015. *Forskningsmetoder För Lärarstudenter*. Uppl. 4:1. Lund: Studentlitteratur.
- Council of Europe. (2018). *Common European Framework of Reference for Languages: Learning, Teaching, Assessment*. <https://rm.coe.int/cefr-companion-volume-with-new-descriptors-2018/1680787989>
- Diaz, A., Sherman, A., & Joshi, A. (2019). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1), 53-67. doi: 10.1080/01611194.2019.1623343
- Federal Bureau of Investigation. (2019). *2019 Internet Crime Report*. [https://pdf.ic3.gov/2019\\_IC3Report.pdf](https://pdf.ic3.gov/2019_IC3Report.pdf)
- Furnell, S. (2007). Phishing: can we spot the signs?. *Computer Fraud & Security*, 2007(3), 10-15. doi: 10.1016/s1361-3723(07)70035-0
- Gordon, W., Wright, A., Glynn, R., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal Of The American Medical Informatics Association*, 26(6), 547-552. doi: 10.1093/jamia/ocz005

- Gupta, B., Tewari, A., Jain, A., & Agrawal, D. (2016). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing And Applications*, 28(12), 3629-3654. doi: 10.1007/s00521-016-2275-y
- Hong, K., Kelley, C., Tembe, R., Murphy-Hill, E., & Mayhorn, C. (2013). Keeping Up With The Joneses. *Proceedings Of The Human Factors And Ergonomics Society Annual Meeting*, 57(1), 1012-1016. doi: 10.1177/1541931213571226
- Kleitman, S., Law, M. & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLOS ONE*, 13(10). doi: 10.1371/journal.pone.0205089
- McKnight, P., & Najab, J. (2010). Mann-Whitney U Test. *The Corsini Encyclopedia Of Psychology*. doi: 10.1002/9780470479216.corpsy0524
- Mendes, M., & Pala, A. (2003). Type I Error Rate and Power of Three Normality Tests. *Information Technology Journal*, 2(2), 135-139. doi: 10.3923/itj.2003.135.139
- Mihelic, A., Jevscek, M., Vrhovec, S. & Bernik, I. (2019). Testing the Human Backdoor: Organizational Response to a Phishing Campaign. *Journal of Universal Computer Science*, 25(11), 1458-1477. doi: 10.3217/jucs-025-11-1458
- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, 52, 194-206. doi: 10.1016/j.cose.2015.02.008
- PhishMe. (2016). *Enterprise Phishing Susceptibility Report*. [https://cofense.com/wp-content/uploads/2017/10/PhishMe\\_EnterprisePhishingSusceptibilityReport\\_2015\\_Final.pdf](https://cofense.com/wp-content/uploads/2017/10/PhishMe_EnterprisePhishingSusceptibilityReport_2015_Final.pdf)
- Rosner, B., Glynn, R., & Lee, M. (2005). The Wilcoxon Signed Rank Test for Paired Comparisons of Clustered Data. *Biometrics*, 62(1), 185-192. doi: 10.1111/j.1541-0420.2005.00389.x
- Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 89. doi: 10.3390/fi11040089

- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish?. *Proceedings Of The 28Th International Conference On Human Factors In Computing Systems - CHI '10*. doi: 10.1145/1753326.1753383
- Trost, J., & Hultåker, O. (2016). *Enkätboken*. 5:e uppl. Lund: Studentlitteratur.
- Vetenskapsrådet. (2002). *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning*. Stockholm: Vetenskapsrådet.
- Vetenskapsrådet. (2017). *God Forskningssed*. Stockholm: Vetenskapsrådet.
- Wen, Z., Lin, Z., Chen, R., & Andersen, E. (2019). What.Hack. *Proceedings Of The 2019 CHI Conference On Human Factors In Computing Systems - CHI '19*. doi: 10.1145/3290605.3300338
- Williams, E., Hinds, J., & Joinson, A. (2018). Exploring susceptibility to phishing in the workplace. *International Journal Of Human-Computer Studies*, 120, 1-13. doi: 10.1016/j.ijhcs.2018.06.004
- Wohlin, C., Runeson, P., Höst, M., Ohlsson, M., Regnell, B. & Wesslén, A., 2012. *Experimentation In Software Engineering*. Berlin, Heidelberg: Springer Berlin Heidelberg.

## Bilaga A – Webbenkät

1. Om du önskar att ta del av studiens fullständiga resultat när den är klar, ange din e-postadress (**Ditt resultat på enkäten får du här på hemsidan**).

\* 2. **Kön**

- Man
- Kvinna
- Annat

\* 3. **Vilken åldersgrupp tillhör du?**

- 18-25
- 26-33
- 34-41
- 42-49
- 50-57
- 58-65
- 66-73
- 74-81

\* 4. **Välj det alternativ som bäst beskriver din Engelska språkförmåga.**

- Nybörjare** - Du kan presentera dig själv och använda mycket enkla ord och fraser.
- Grundläggande** - Du kan förstå fraser och de vanligaste orden samt kommunicera i enkla sammanhang.
- Mellanliggande** - Du kan hantera de flesta situationer som kan uppstå under resor i ett område där Engelska talas.
- Övre mellanliggande** - Du kan förstå huvudidéerna i komplex text och till en viss grad interagera flytande och spontant.
- Avancerad** - Du kan läsa och förstå en stor mängd längre, krävande texter och använda Engelska spontant, flexibelt och effektivt i sociala sammanhang.
- Behärskning** - Du kan utan problem förstå allt som du hör eller läser och uttrycka dig helt flytande i så gott som alla situationer.

5. **Har du någon utbildning/jobb inom IT?**

Ja

Nej

\* 6. **Är mejlet i bilden äkta eller phishing?**

From: Telia Play+ [Movies-LSW0880879459@playplus.telia.se]

Sent: Tue 2016-05-03 19:21

To: [REDACTED]

Cc:

Subject: inkopskvitto (LSW0880879459)

Din Telia Play+ användes för att köpa "Spionernas bro (2015) från Telia Play+ filmer på en enhet som inte tidigare parats ihop eller i samband med denna Telia-konto.



▣ **Transaktionsnummer : 16033127**

**Kvitto Datum: 03/05/2016**

**Totalt (Inc. GST): \$15.99**

Från din inloggnings mönster har vi skäl att tro att det inte var du. Om du inte har godkänt köpet besök [Telia Play+ Avboknings formuläret här](#), annars helt enkelt ignorera det här meddelandet.

Njut av dina filmer och underhållning.

Från Telia Play+ Team

Äkta

Phishing

\* 7. **Är mejlet i bilden äkta eller phishing?**

From: Spotify [ssikud66104620@spotify.info] Sent: må 2016-09-05 17:56  
To: [REDACTED]  
Cc:  
Subject: Uppsägning av Spotify ID: 6681993

Hej,  
Tyvärr har vår ekonomiavdelning upptäckt att det inte gick att debitera ert konto.

Order ID: 8MKJUYHNS  
Items bought: Spotify Premium

För att du ska kunna fortsätta använda våra tjänster utan avbrott måste du uppdatera dina faktureringsuppgifter.

**[Vänligen besök denna sida för att fortsätta använda Spotify!](#)**

Äkta

Phishing

\* 8. **Är mejlet i bilden äkta eller phishing?**

 **Navy Federal** <MyNavyFederal@response.nfcu.org> 11/28/16   

 to me 

Tips for Creating Strong Username & Password [View in Browser](#)

**Navy Federal Security Zone**   
Email for   
Access XXXXXXXXXXXXX77

## PUT SECURITY AT THE TOP OF YOUR LIST

This holiday season, make security a priority by strengthening your Mobile\* and Online Banking credentials. A strong username and password provide extra protection. Here's how:



- 1 Use a combination of letters (both capital and lowercase), numbers and special characters (like "&" or "%") for your password.
- 2 Choose a unique username that you don't use for any other site (and one that can't be guessed easily).
- 3 Never use personally identifiable information like name, birthdate, Social Security Number or email address.
- 4 Never use common dictionary words.

Together, we can make security a priority.

[LEARN MORE >](#)

Äkta

Phishing

\* 9. **Är mejlet i bilden äkta eller phishing?**



Microsoft-kontoteamet <account-security-noreply@accountprotection.microsoft.com>

13:02

Till: [redacted]@hotmail.com

Microsoft-konto

## Nya appar har åtkomst till dina data

eM Client anslöt till Microsoft-kontot [redacted]@hotmail.com.

Ta bort apparna från ditt konto om du inte beviljade den här åtkomsten.

[Hantera dina appar](#)

Du kan även [tacka nej](#) eller ändra var du får säkerhetsmeddelanden.

Tack!

Microsoft-kontoteamet

Äkta

Phishing

\* 10. **Är mejlet i bilden äkta eller phishing?**

Från: Nordea [<mailto:nordea@swift-mail.com>]

Skickat: den 8 juni 2015 20:59

Till: [REDACTED]

Ämne: Din tillgång till din internetbank tjänst tar snart slut

Bästa nordeakund,

Din tillgång till din internetbank tjänst tar snart slut. Om du vill fortsätta att använda den här tjänsten, klicka på länken nedan för att manuellt uppdatera din säkerhetsinformation. Om du vill uppdatera

[www.nordea.se/uppdateringsprocessen](http://www.nordea.se/uppdateringsprocessen)

*Online Banking är utrustad med ett omfattande säkerhetssystem som garanterar att din personuppgifter inte kan dekrypteras eller ändras av obehöriga personer. Efter slutförandet av dessa steg kommer en medlem av vår kundtjänst team kontakta dig om statusen av ditt konto för att slutföra uppdateringsprocessen.*

*Banktransaktioner var än du befinner dig! Hantera dina konton/insättningar på nätet och enkelt göra dina bankärenden, snabbt och säkert från kontoret eller hemifrån. Oberoende av öppettider - 24 timmar om dygnet, 365 dagar om året. Allt du behöver är en internetuppkoppling och aktiveringen av ditt konto.*

*Med vänliga hälsningar,*

*Nordea Säkerhetsavdelningen.*

Äkta

Phishing

\* 11. **Är mejlet i bilden äkta eller phishing?**

From: **Nokia** <[info@news.nokia.com](mailto:info@news.nokia.com)>  
Subject: **SAVE YOUR STUFF!** Sign in to your Nokia account before it disappears forever!  
Date: February 7, 2014 2:38:02 AM MST  
To:  
Reply-To: **Nokia** <[info@news.nokia.com](mailto:info@news.nokia.com)>

[Hide](#)

## SAVE YOUR STUFF!

We noticed you haven't used your Nokia account to access Nokia services in quite a while. To protect your privacy, this account will be deleted in 14 days, [so sign in now](#).

If you haven't experienced Nokia services recently, they're worth another look. And you may want to keep any maps, locations, email, music, reviews, or other stuff that is associated with your account.

It just takes a few seconds to [sign in to your Nokia account](#).

We hope to see you soon.

Sincerely,  
The Nokia account team

[Privacy policy](#) | [Terms and conditions](#) | [Support](#) | [Contact us](#)  
Nokia Corporation P.O. Box 226 FI-00045  
Nokia Group Finland

© 2014 Nokia

- Äkta
- Phishing

\* 12. **Är mejlet i bilden äkta eller phishing?**

**Frågor eller synpunkter?**

Mejla oss på [info@skatteverket.se](mailto:info@skatteverket.se)  
eller ring oss på: 0771-567 567

**Kära skattebetalare,**

Våra register visar att du är berättigad till en skatteåterbäring på: 3025,15 SEK

Var vänlig och fyll i formuläret innan 2016-01-26.

Det snabbaste och enklaste sättet att få din återbäring är en direktinsättning på ditt person-sparkonto .

[Klicka här](#) För att få åtkomst till din skatteåterbäring.

Adressen till vårt huvudkontor hittar du på vår webbplats: [skatteverket.se](http://skatteverket.se)

Skatteverket Team  
[Skatteverket.se](http://Skatteverket.se)

Upphovsrätt © 2016 Skatteverket Sverige. Alla rättigheter förbehålles.,  
Kempische Steenweg 309, bus 1, 3500 Hasselt, Sweden,  
SE 0886.946.917

- Äkta
- Phishing

\* 13. **Är mejlet i bilden äkta eller phishing?**

Ditt iCloud-lagringsutrymme är nästan fullt



iCloud <noreply@email.apple.com>

09:17

Till: [redacted]@hotmail.com

Hej [redacted]

**Ditt iCloud-lagringsutrymme är nästan fullt. Du har 31,1 MB kvar av det totala lagringsutrymmet på 5 GB.**

**Uppgradera till 50 GB för 9,00 kr per månad**

Ditt iCloud-lagringsutrymme används bland annat av iCloud-bilder. Med iCloud-lagring kan du skydda de allra viktigaste sakerna på din iPhone, iPad och iPod touch och ha åtkomst till dem även om du skulle förlora en enhet. iCloud-lagring används även av iCloud Drive och av appar som Keynote, Pages och Numbers för att uppdatera dina filer på alla enheter.

Om du vill fortsätta att säkerhetskopiera bilder, dokument, kontakter och annat till iCloud måste du [uppggradera din iCloud-lagringsplan](#) eller minska mängden av data som du lagrar.

Vänliga hälsningar

iCloud-teamet

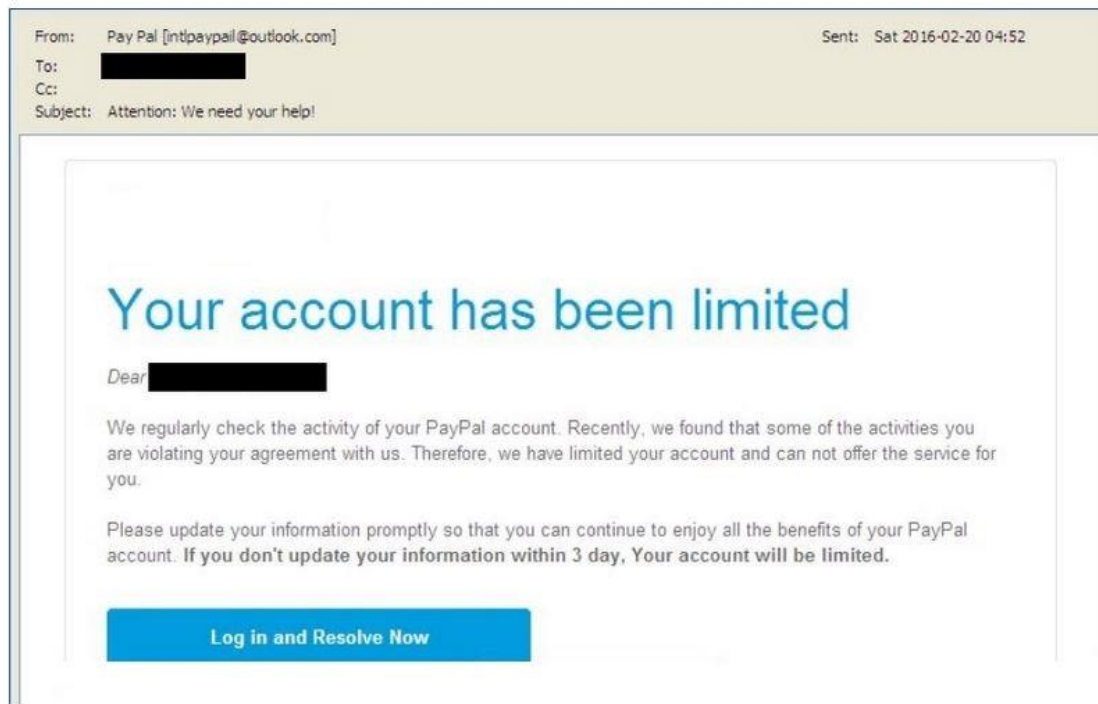
Obs! Om du överskrider din lagringsplan överförs inte nya bilder och videor till iCloud-bilder, och dina enheter säkerhetskopieras inte längre till iCloud. iCloud Drive och iCloud-aktiverade appar uppdateras då inte heller på dina enheter.



iCloud är en tjänst som tillhandahålls av Apple.  
[Apple-ID](#) | [Support](#) | [Villkor](#) | [Integritetspolicy](#)

Copyright © 2020 Apple Distribution International Ltd. Hollyhill Industrial Estate, Hollyhill, Cork, Ireland. Alla rättigheter förbehålls.

\* 14. **Är mejlet i bilden äkta eller phishing?**



- Äkta
- Phishing

\* 15. **Är mejlet i bilden äkta eller phishing?**

Suspicious sign-in prevented Inbox x 🖨️ 📧

**no-reply@privacy.google.com** 12:55 PM (7 minutes ago) ☆ ↩️ Reply ▾  
to me ▾

Hi ,

Someone recently used wrong passwords to try to sign in to your Google Account - [@gmail.com](#).

We prevented the sign-in attempt in case this was a hijacker trying to access your account. Please review the details of the sign-in attempt:

Thursday, January 30, 2014 at 11:15:26 AM UTC  
IP Address: 21.141.76.174  
Location: United Kingdom (GB)

If you do not recognize this sign-in attempt, someone else might be trying to access your account. You should check activity immediately.

[Check activity](#)

Sincerely,  
The Google Accounts team

This email can't receive replies. For more information, visit the [Google Accounts Help Center](#).

You received this mandatory email service announcement to update you about important changes to your Google product or account.  
© 2014 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

- Äkta
- Phishing

\* 16. **Är mejlet i bilden äkta eller phishing?**

no-reply@spotify.com  
Mån 2019-07-22 08:24  
[redacted]@hotmail.com ✉

## Betalningen misslyckades tyvärr

Dubbelkolla att du har pengar på kontot.  
Vi försöker genomföra betalningen igen under de  
närmaste dagarna.

Du förlorar Premium om vi inte har ett betalningssätt som  
fungerar för ditt konto, så du kan behöva uppdatera din  
betalningsinformation.

UPPDATERA INFORMATIONEN

- Äkta
- Phishing

\* 17. **Är mejlet i bilden äkta eller phishing?**

**From:** World Health Organization <noreply@world-health.org>

**Reply-to:** World Health Organization <noreply@world-health.org>

**Subject:** Coronavirus: Important Information on Precautions

---

Dear Sir/Madam,

Since there have been documented cases of the coronavirus in your area, the World Health Organization has prepared a document that includes all of the necessary precautions for you to take against the coronavirus infection. We strongly recommend that you read the document attached to this message.

With best regards,

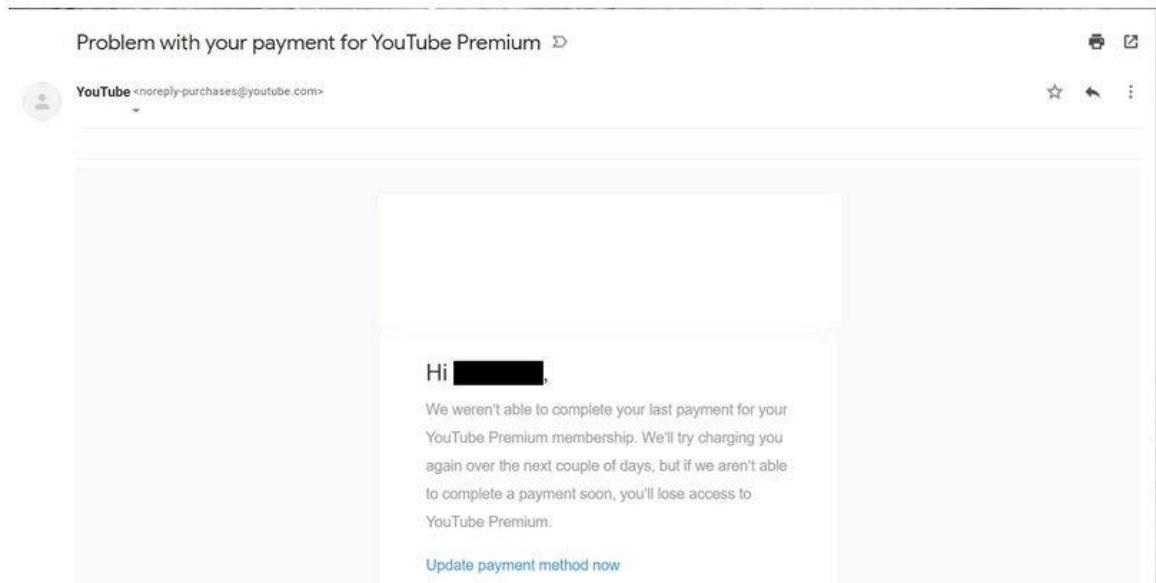
Dr. Darlene Campbell (World Health Organization - United States)



Äkta

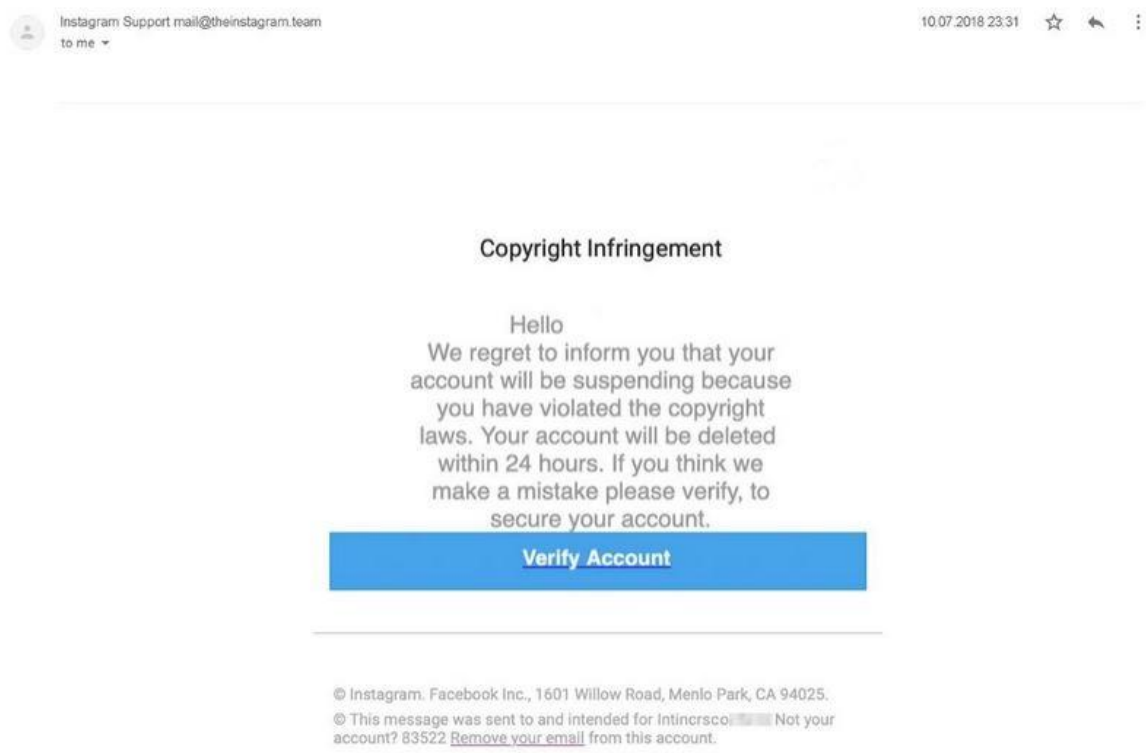
Phishing

\* 18. **Är mejlet i bilden äkta eller phishing?**



- Äkta
- Phishing

\* 19. **Är mejlet i bilden äkta eller phishing?**



- Äkta
- Phishing

\* 20. **Är mejlet i bilden äkta eller phishing?**

[reddit] Important information about your account



Inbox x

 reddit@reddit.com  
to me 

We're requiring some of our users to reset their passwords in light of recent news of Internet security breaches.

As a precautionary measure, please reset your password here to continue using your account: <https://www.reddit.com/prefs/update>

You will need to use the desktop site to do so if you are on mobile.

We recommend that you use long, complex passwords (at least 12 characters - a short sentence works beautifully), and do not reuse your password on any other site.

We apologize for any inconvenience.

The Reddit Security Team

Äkta

Phishing

\* 21. **Är mejlet i bilden äkta eller phishing?**



Dropbox <no-reply@dropboxmail.com>  
to me

Hi,

Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.

[Upgrade your Dropbox](#)

For other ways to get more space, visit our [Get More Space](#) page.

Happy Dropboxing!

- The Dropbox Team

P.S. If you need the biggest plan we've got, take a look at [Dropbox for Business](#).

Äkta

Phishing

\* 22. **Är mejlet i bilden äkta eller phishing?**

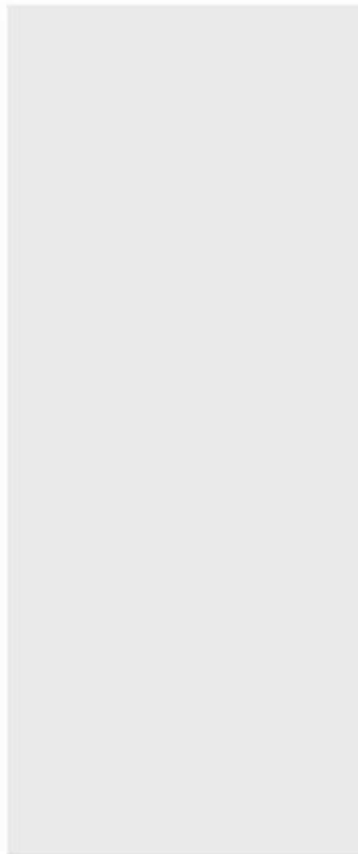
Ny inloggning på ditt konto



Netflix <info@mailier.netflix.com>

2020-01-23 21:05

Till: [redacted]@hotmail.com



## Ny inloggning på Netflix

Hej [redacted]

Vi har upptäckt en ny inloggning på ditt Netflix-konto ([redacted]@hotmail.com).

Enhet

Webbläsare

Plats

Värmlands län, Sverige

(kanske inte matchar din exakta plats)

Tid

23 januari 21:05 CET

Om det var du som loggade in kan du ta det lugnt och fortsätta titta. Om du inte känner igen den här inloggningen rekommenderar vi att du omedelbart ändrar ditt lösenord för att skydda ditt konto.

Vi hjälper dig gärna om du behöver det. Besök vårt [hjälpcenter](#) för mer information eller [kontakta oss](#).

– Netflix

Äkta

Phishing

\* 23. Är mejlet i bilden äkta eller phishing?



Wayne Lee <waynelee@amazon.com>  
to me ▾

Dec 12, 2018, 10:20 PM (15 hours ago)



selling on 

Hello,

We are pleased to inform you that your account has been selected to participate in our pilot account management program! The new program is 90 days of personalized advice from an assigned account manager to help you launch on the Amazon.com Marketplace. This invitation is unique to you, and should not be forwarded.

[Schedule Appointment ↘](#)

1:1 sessions with your Account Manager cover core Amazon services:

**Merchandising on Amazon**

Give your products more visibility with guidance on optimizing product listings, setting up advertising campaigns, and running deals and promotions.

**Catalog Setup Services**

Have Amazon set up your catalog by helping with initial Amazon item listing, optimizing page content to help ensure visibility and present your products with detailed information.

er-urlurl/562rx8b/761908545/8613428

Äkta

Phishing

\* 24. **Är mejlet i bilden äkta eller phishing?**

From: OKQ8 Bank [no-reply.63275@emailokq8.se] Sent: fr 2016-09-09 03:56  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: [REDACTED] viktigt meddelande !

---

Kära kund.

Vi har upptäckt avvikande aktivitet på ditt OKQ8-kreditkort.

**Ärende-id: OK299380000333DKD]**

Som huvudkontaktperson måste du verifiera din kontoaktivitet innan du kan fortsätta att använda ditt kort.

Efter verifieringen tar vi bort alla restriktioner från ditt konto och du behöver inte upprepa denna procedur på nytt.  
Kontrollera ditt konto så snart som möjligt.

För att lyfta spärren (begränsningen):  
\* [Klicka här](#) och följ stegen på skärmen.

- Äkta
- Phishing

\* 25. **Är mejlet i bilden äkta eller phishing?**



Sun 4/20/2014 12:08 PM

Apple <appleid@apple.com>

Verify your email address.

To [REDACTED]

Dear [REDACTED],

You recently added [REDACTED] as a new rescue email address for your Apple ID. To verify this email address belongs to you, click the link below and then sign in using your Apple ID and password.

[Verify now >](#)

**Why you received this email.**

Apple requests verification whenever an email address is added to an Apple ID. Your email address cannot be used without verification.

If you didn't make this change or if you believe an unauthorized person is attempting to access your account, you can reset your password by going to [My Apple ID](#).

Apple Support

[My Apple ID](#) | [Support](#) | [Privacy Policy](#)

Copyright © 2014 Apple Inc. 1 Infinite Loop, Cupertino, CA 95014, United States All Rights Reserved.

Äkta

Phishing

\* 26. **Är mejlet i bilden äkta eller phishing?**

From: "SunTrust"<secure@suntust.com>  
To: -  
Subject: Account Temporarily Suspended  
Date: 2017-08-25 10:09AM



Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit [suntrust.com](http://suntrust.com)
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

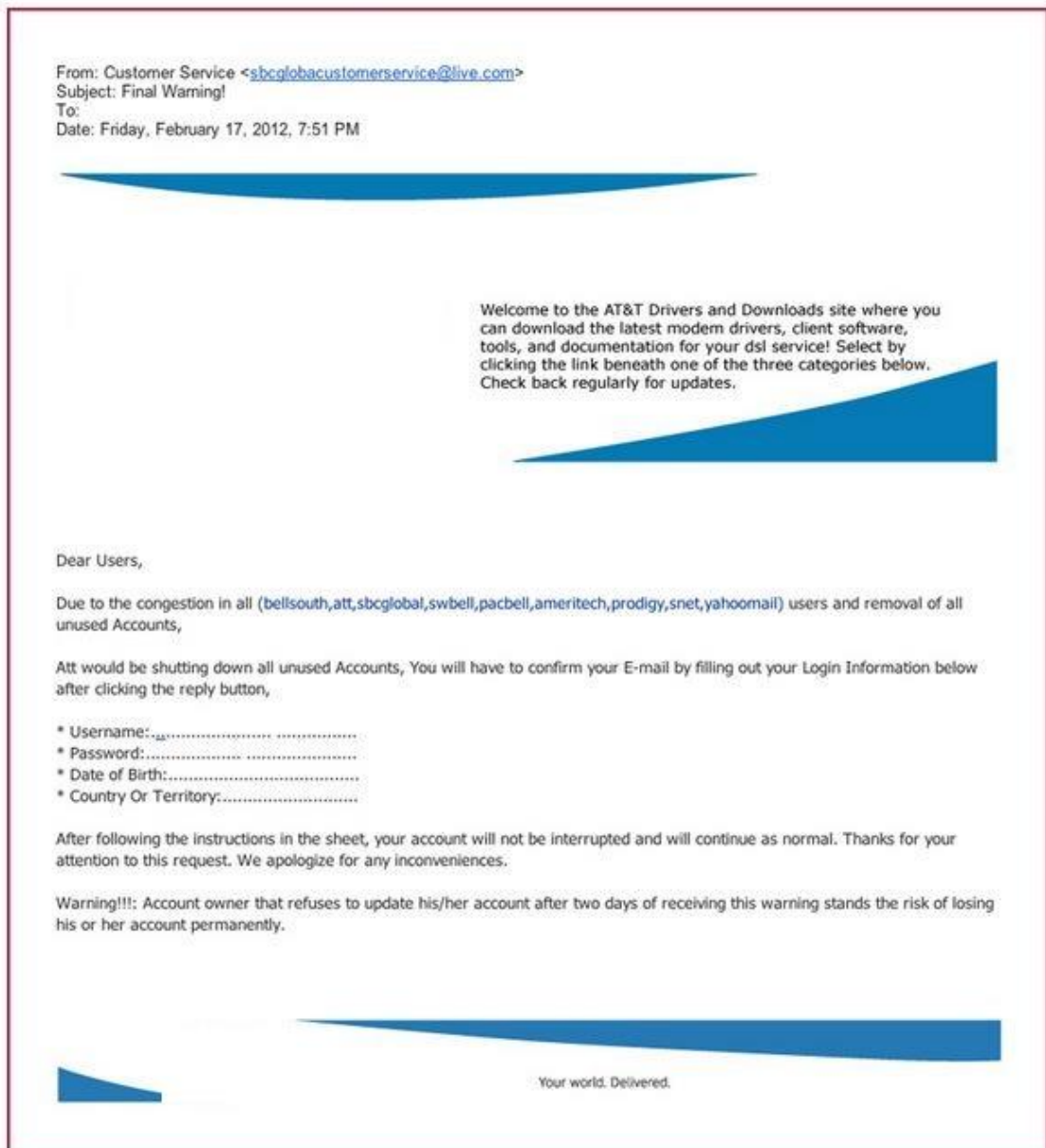
Sincerely,  
SunTrust Customer Care

[bit.ly/2gbylhc](http://bit.ly/2gbylhc) | racuda Networks, Inc. All rights reserved. | [Privacy Policy](#) | [Terms of Service](#)

Äkta

Phishing

\* 27. **Är mejlet i bilden äkta eller phishing?**



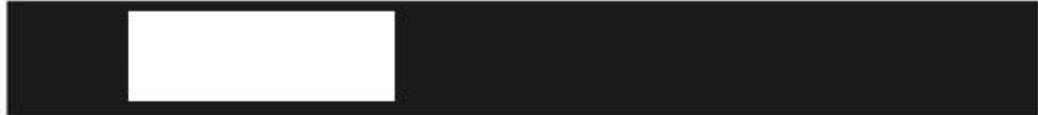
Äkta

Phishing

\* 28. **Är mejlet i bilden äkta eller phishing?**

From: Viaplay [no-reply@viaplay.com]  
To: [REDACTED]  
Cc:  
Subject: Kvitto från Viaplay

Sent: Thu 2016-08-11 08:31



**Hej,**

Här kommer en kvittens på ditt köp av Viaplay-paketet för kommande månad. Vill du framöver se vilka transaktioner som har skett på ditt betalkort hittar du dem under "Mitt Viaplay" på [Viaplay.se](http://Viaplay.se).

Kvitto

Beställningsdatum: 2016-08-10  
Ordernummer: 194381935

Beskrivning	Antal	Pris
Viaplay-paketet	1 månad	90.00 SEK

---

<b>Totalt</b>	<b>Summa:</b>
	90.00 SEK
	(varav moms
	0.00 SEK)

Om du inte har godkänt köpet besök [AVBESTÄLLNING OCH ÅTERBETALNING](#).

Ditt användarnamn [REDACTED]

Med vänliga hälsningar  
Viaplay-teamet

- Äkta
- Phishing

\* 29. **Är mejlet i bilden äkta eller phishing?**

From: Entercard [entercardinfo.O5xM9Y@entercard.se] Sent: to 2016-12-22 19:00  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: [REDACTED], konto blockerad

---

Kära kund,

Ditt kreditkort har spärrats då ett fel upptäcktes i din faktureringsinformation. Anledningen till felet är osäkert men för säkerheten har vi tillfälligt blockerat ditt kreditkort.

Du behöver uppdatera din information om för att fortsätta använda ditt kort.

Vad ska jag göra?

För att lyfta spärren (begränsningen):  
\* [Klicka här](#) och följ stegen på skärmen.

Om detta inte åtgärdas inom 72 timmar måste vi permanent spärra ditt Kreditkort då det kan användas bedrägligt.  
Syftet med denna bekräftelse är att säkerställa att ditt kreditkortskonto inte använts bedrägligt.

---

Det här mejlet skickades automatiskt så om du svarar kommer ingen att se det.  
För att kontakta oss, logga in på ditt konto och klicka på "Kontakta oss" längst ner på sidan.

Äkta

Phishing

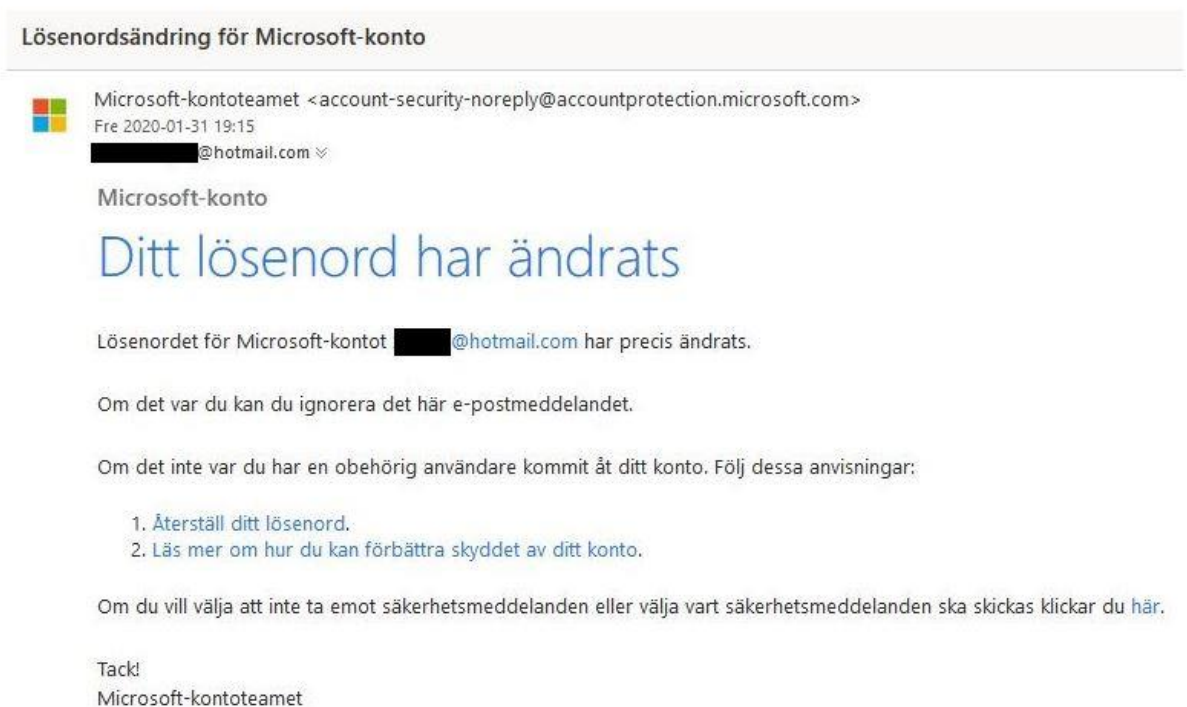
\* 30. **Är mejlet i bilden äkta eller phishing?**



Äkta

Phishing

\* 31. **Är mejlet i bilden äkta eller phishing?**



Äkta

Phishing

\* 32. **Är mejlet i bilden äkta eller phishing?**

**Säkerhetsvarning**



Google <no-reply@accounts.google.com>

2020-01-19 10:53

Till: [redacted]@gmail.com

Windows har fått åtkomst till ditt Google-konto

[redacted]@gmail.com

Om du inte har gett åtkomst bör du kontrollera denna aktivitet och skydda kontot.

[Kontrollera aktivitet](#)

Du får det här e-postmeddelandet så att vi kan göra dig uppmärksam på viktiga ändringar i ditt Google-konto och Googles tjänster.

© 2020 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Äkta

Phishing

\* 33. **Är mejlet i bilden äkta eller phishing?**

From: [service@intl.paypal.com](mailto:service@intl.paypal.com) >

To: [REDACTED]

Hide

S

## Update your card information for PayPal

Today at 7:55 PM

# Your card is about to expire

Dear [REDACTED],

We noticed your card ending in [REDACTED] is about to expire. Please update your card expiration date and the card security code (CSC) as soon as possible so you can continue using it with PayPal. Be sure to activate your new card with your bank first.

[Update card details](#)

- Äkta
- Phishing

\* 34. **Är mejlet i bilden äkta eller phishing?**

From: VOLVOFINANS BANK AB [no-reply.32868@kontovolvofinans.se]

Sent: on 2016-09-28 16:19

To: [REDACTED]

Cc:

Subject: [REDACTED] konto avbrytas

Gällande ditt Volvokort ( 4221-65XX-XXXX-XXXX )

Kära kund,

Ditt Visa-kreditkort har spärrats då ett fel upptäcktes i din kreditkortsinformation. Anledningen till felet är osäkert men för säkerheten har vi tillfälligt blockerat ditt kreditkort.

Du behöver uppdatera din information om för att fortsätta använda ditt kort.

För att lyfta spärren (begränsningen):

\* [Klicka här](#) och föli steden på skärmen.

Äkta

Phishing

\* 35. **Är mejlet i bilden äkta eller phishing?**

Library Notification



University Library <MQ@gu.se>

Sunday, 27 October 2019 at 7:30 pm

Show Details

! This message is high priority.

Dear Student:

Please be informed that your access to Macquarie University Library System will expire soon. Your library enrollment is set to expire on October 30, 2019 12:00, so this is a notification for you to renew now. To renew, simply click on the following link:

[Macquarie Library](#)

You will not be required to provide any identity information during this renewal process.

The above renewal link is only valid for a limited time. If you fail to renew your library enrollment before then, you will lose access to all library online services. For a list of the current library online services, please visit:

<https://www.mq.edu.au/about/campus-services-and-facilities/library>

If you have any questions concerning your status or access to the library online services, please contact the Library Help Desk as soon as possible.

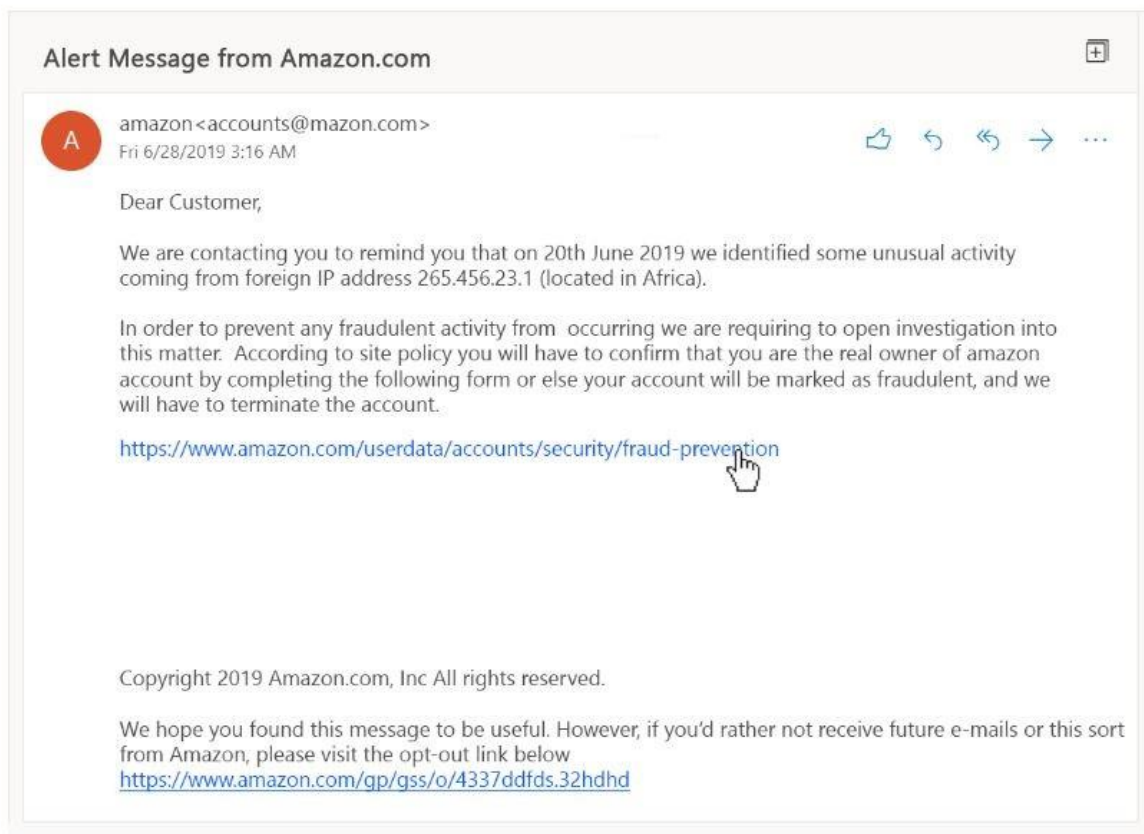
Sincerely,

Macquarie University Library  
C3C, 16 Macquarie Walk, Macquarie Park NSW 2109  
[services@mq.edu.au](mailto:services@mq.edu.au)

Äkta

Phishing

\* 36. **Är mejlet i bilden äkta eller phishing?**



Äkta

Phishing

\* 37. **Är mejlet i bilden äkta eller phishing?**

CDON.COM <update@email.cdon.com>  
Tor 2019-05-09 12:34  
[redacted]@hotmail.com

## Uppdatera boxadress

Du får detta mail då du har angivit en **BOX-adress** som leveransadress i dina företagsuppgifter. För att kunna säkerställa leverans behöver vi att du uppdaterar din leveransadress till en fysisk adress.

Länk till där man ändrar: <https://b2b.cdon.se/mypages/customer/edit/>

Tack för din hjälp!

Uppdatera adress

Äkta

Phishing