Simrishamns kommun

Rapport: Informationssäkerhet i praktiken
Mars 2023

Sammanfattning

Granskningens syfte är att, på uppdrag av de förtroendevalda revisorerna, bedöma om kommunstyrelsen har säkerställt en tillräcklig intern kontroll avseende kommunens arbete med IT- och informationssäkerhet inom området falska e-postmeddelanden. Detta undersöks genom att testa utbildning och medvetenhet hos medarbetarna inom Simrishamns kommun, vilket utförs genom att simulera ett angrepp via e-post, där kommunens tekniska skydd har kopplats bort. Följande revisionsfrågor har legat till grund för granskningen:

- Hanterar Simrishamns kommuns medarbetare hotet från attacker genom falska email, så kallad phishing (nätfiske), på ett ändamålsenligt sätt?
- Har Simrishamns kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av den testade personalen under den simulerade attacken?
- Är riktlinjer för hantering och rapportering av falska email och andra incidenter kända hos personalen?

Granskningen genomfördes från december 2022 till mars 2023. EY utformade och genomförde granskningen tillsammans med representanter från kommunen i syfte att uppnå en så stor nytta som möjligt för verksamheten. Metoden som använts bygger på EY:s beprövade metodik för att genomföra en simulerad phishing-attack. Tre huvudområden analyserades: 1) Mottagare som klickat på länken i e-postmeddelandet, 2) Mottagare som uppgav användarinformation på landningssidan, samt 3) Mottagares medvetenhet kring informationssäkerhet och phishing. Dessa områden jämfördes sedan mot på förhand definierade acceptansnivåer och med vad EY anser är en godtagbar standard i offentlig sektor.

Baserat på genomförd granskning bedömer EY att det finns brister gällande utbildning och medvetenhet inom informationssäkerhet i Simrishamns kommun. Granskningsresultatet visar att kommunen ligger på en nivå under det man enligt EY bör förvänta sig av jämförbara organisationer inom den kommunala sektorn. Slutsatsen baseras på den typ av verksamhet som bedrivs och på känslighetsgraden av den information, exempelvis personuppgifter, som behandlas. I relation till acceptansnivåerna löper Simrishamns kommun en hög risk att utsättas för en fullbordad phishing-attack. Kommunstyrelsen rekommenderas därför att vidta åtgärder för att informera och tydliggöra relaterade styrdokument och riktlinjer, konkretisera rapporteringsvägar, och stärka utbildning och medvetenhet hos medarbetarna. En förbättrad motståndskraft mot phishing kan bidra till att förluster av känslig information, negativt rykte eller andra betydande konsekvenser minskar. Baserat på granskningen har EY valt att presentera fyra övergripande rekommendationer:

- Tydliggör och informera om rutiner för rapportering av misstänkta e-postmeddelanden.
- Genomför teoretiska och praktiska utbildningar avseende identifiering av phishing.
- Målgruppsanpassa utbildningsinsatser.
- Utbilda nyanställda i riktlinjer för informationssäkerhet och phishing.

Innehållsförteckning

1. Bakgrund

Simrishamns kommun hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare. Digitaliseringen medför samtidigt risker som uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

Kommunens revisorer har identifierat risker relaterat till kommunens övergripande arbete med IT- och informationssäkerhet. Revisorerna har därför valt att genomföra en granskning för att testa hur väl kommunens riktlinjer och rutiner med IT- och informationssäkerhet har kommunicerats till medarbetarna i praktiken.

Granskningen genomförs genom att EY simulerar en attack där falska e-postmeddelanden skickas ut till medarbetarna, en så kallad phishing- eller nätfiskeattack. Eftersom det är medarbetarnas motståndskraft som testas har det tekniska skyddet kopplats bort för denna simulering. Genom ett fullgott informationssäkerhetsarbete från kommunens sida, bör medarbetarna kunna identifiera ett sådant angrepp, och veta hur de ska agera för att hantera och rapportera den simulerade attacken med bibehållen säkerhet. Med hjälp av resultatet på hur många som agerade korrekt kan revisorerna få en bild av hur medvetna medarbetarna är och hur väl utbildning fungerar i praktiken.

1.1 Phishing och nätfiske

Ökad digitalisering leder till ökade informationssäkerhetsrisker. Cyberkriminella attackerar inte enbart en organisations tekniska miljö utan väljer i hög utsträckning att rikta in sig på människorna i organisationen. Cyberkriminella ägnar sig åt social manipulation genom att utnyttja mänskliga svagheter såsom rädsla och förtroende för att komma åt känslig information eller för att sprida skadlig kod. Något som riskerar att allvarligt skada organisationer, deras intressenter och samhället i stort. Sedan Covid-19-pandemin har EY sett en ökning av denna typ av cyberkriminalitet, särskilt genom phishing. Det är svårt att fullt ut skydda en organisation mot phishing-attacker enbart genom tekniska hjälpmedel. Detta innebär att den mänskliga aspekten blir avgörande för att säkerställa ett adekvat skydd av en organisations tillgångar och för att uppfylla lagkrav om informationssäkerhet och integritet.

En fullbordad phishing-attack kan innebära stora konsekvenser för en organisation, både ekonomiskt och i form av försämrat anseende och rykte. Det är därmed viktigt att vara proaktiv för att hantera det ökade hotet från phishing. Ett viktigt tillvägagångssätt för detta är att hålla medarbetare inom en organisation medvetna om hotet från phishing, och ge dem kunskapen att kunna identifiera falska e-postmeddelanden. Medarbetare bör även ha en tydlig rapporteringsväg att följa för att rapportera misstänkta e-postmeddelanden. Ett annat sätt att minska riskerna med den här typen av cyberattacker är att kontinuerligt genomföra medvetenhetsträning inom informationssäkerhet. Detta för att medarbetare ska kunna upptäcka och reagera på försök till nätfiske.

1.2 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om det kommunstyrelsen har säkerställt en tillräcklig intern kontroll avseende kommunens arbete med IT- och informationssäkerhet inom området falska e-postmeddelanden. Detta undersöks genom att testa utbildning och medvetenhet hos medarbetarna inom Simrishamns kommun.

Följande revisionsfrågor har legat till grund för granskningen:

- Hanterar Simrishamns kommuns personal hotet från attacker genom falska email, så kallad phishing (nätfiske), på ett ändamålsenligt sätt?
- Har Simrishamns kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av den testade personalen under den simulerade attacken?
- Är riktlinjer för hantering och rapportering av falska email och andra incidenter kända hos personalen?

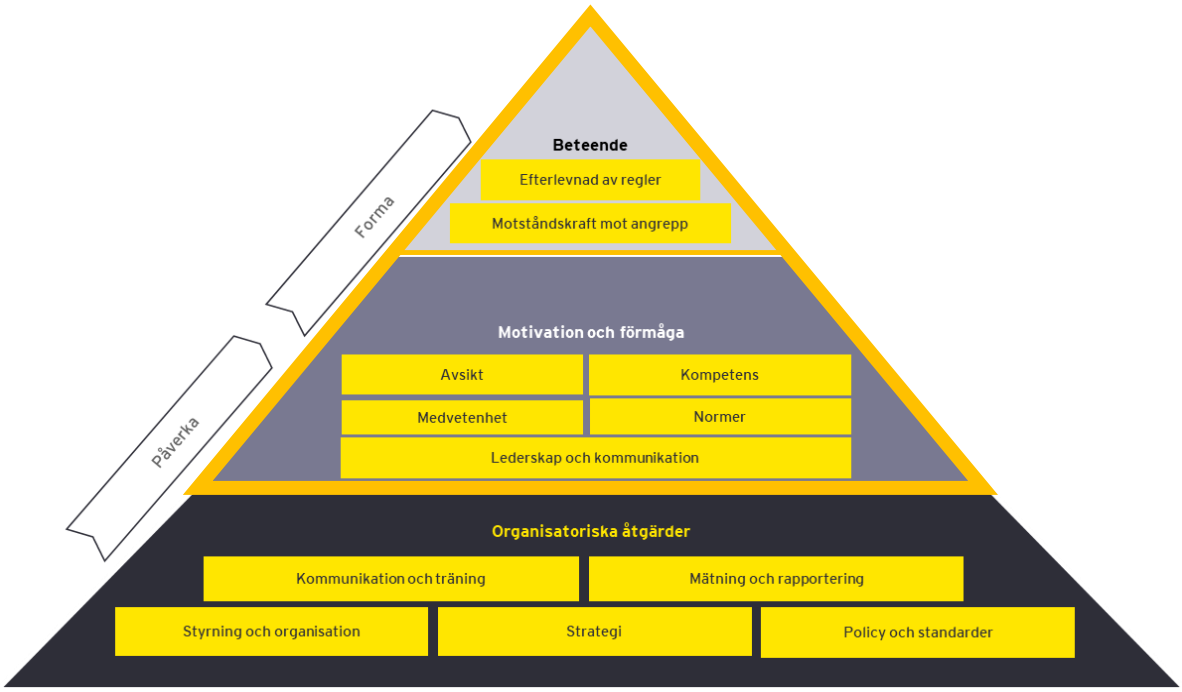
1.3 Avgränsningar

Granskningen är avgränsad till att ge en bild av hur sårbar kommunen är för attacker riktade mot medarbetarna via e-postmeddelanden. Det ges alltså inte någon helhetsbild av kommunens fullständiga arbete inom IT- och informationssäkerhet utan syftet är ge en mer detaljerad bild av ett begränsat område. Ingen teknisk testning har utförts för att granska effektiviteten i kommunens skalskydd, det vill säga hur väl tekniska hjälpmedel fungerar för att identifiera och stoppa falska e-postmeddelanden.

1.4 Metod och genomförande

Granskningen bygger på EY:s etablerade ramverk för hur en organisation arbetar med informationssäkerhet. *Figur 1* nedan visar hur organisatoriska åtgärder som exempelvis kommunikation och utbildning, styrning, samt riktlinjer ligger till grund för nivån av informationssäkerheten i en organisation. De organisatoriska åtgärderna påverkar sedan i sin tur motivationen och förmågan hos anställda att agera i enlighet med de riktlinjer organisationen fastställt. Motivationen och förmågan hos anställda baseras på flera olika faktorer som ledarskap och kommunikation, avsikt, samt medvetenhet och kompetens kring informationssäkerhet. Motivationen och förmågan hos medarbetarna i Simrishamns kommun har i denna granskning utvärderats genom en enkät som distribuerades efter genomförd övning. Enkätens syfte var även att mottagarna själva skulle reflektera över deras medvetenhet, kunskap och beteende kring informationssäkerhet.

Motivationen och förmågan hos medarbetare i en organisation formar i sin tur deras beteende relaterat till informationssäkerhet, närmare bestämt hur väl man efterlever regler och hur stark motståndskraften är mot ett potentiellt angrepp inom organisationen. Beteendet hos medarbetare i Simrishamns kommun har i denna granskning utvärderats genom att utföra en simulerad phishing-attack. Notera att granskningen i sin helhet huvudsakligen fokuserar på de två översta delarna av ramverket: beteende samt motivation och förmåga.



Figur 1: EY:s ramverk för bedömning av en organisations informationssäkerhet

Nedan följer en mer detaljerad beskrivning av EY:s metodik för att utföra en phishing-övning och en detaljerad beskrivning av hur övningen genomfördes.

1.4.1 Metod

EY använder en beprövad metodik för att genomföra och analysera en simulerad phishing-attack. Övningen sätts upp med hjälp av ett verktyg som används för att skicka ut ett e-postmeddelande till den definierade målgruppen och för att samla in data kring hur mottagarna hanterat meddelandet. Insamlad information jämförs sedan mot på förhand definierade acceptansnivåer och vad EY anser är en godtagbar standard i offentlig sektor. Den information som ligger till grund för granskningen har samlats in av EY i möten med utvalda nyckelpersoner från IT-avdelningen i Simrishamns kommun.

För att besvara revisionsfrågorna har EY analyserat tre huvudområden enligt nedan:

- **Mottagare som klickade på länken i e-postmeddelandet** – EY har granskat hur många mottagare av det förfalskade e-postmeddelandet som klickade på den inbäddade länken till landningssidan (internetsida). Detta för att få en förståelse för kommunens motståndskraft mot hotet av phishing, samt hur god kunskapsnivån hos kommunens medarbetare är för att kunna identifiera ett e-postmeddelande från en falsk avsändare. EY bedömer att detta är ett viktigt område att granska då riskerna för att cyberkriminella kan utvinna känslig information, implementera skadlig kod, eller attackera en organisations IT-infrastruktur ökar avsevärt om en mottagare klickar på en skadlig länk.

- **Mottagare som uppgav användarinformation på landningssidan** – EY har granskat hur många mottagare av det förfalskade e-postmeddelandet som initialt klickade på länken inbäddad i e-postmeddelandet för att sedan uppge användarinformation på den förfalskade landningssidan. Detta för att skapa en förståelse för hur stark kommunens motståndskraft är mot angrepp av phishing, samt för att mäta kunskapsnivån hos kommunens medarbetare att kunna identifiera en förfalskad landningssida från en okänd domän. EY bedömer att detta är ett viktigt område att granska då riskerna för att cyberkriminella kan utvinna känslig information och ta sig in i en organisations IT-infrastruktur ökar avsevärt om en medarbetare delar med sig av sin användarinformation.

- **Mottagares medvetenhet om informationssäkerhet och phishing** - EY har med hjälp av kommunen distribuerat en enkät med syftet att skapa sig en uppfattning om motivationen och kunskapen relaterat till denna typ av cyberhot hos mottagarna av e-postmeddelandet. Enkäten omfattar frågor kring e-postmeddelandet som användes i simuleringen och säkerhetskulturen på kommunen i form av utbildning och medvetenhet, styrande dokument och rapportering av säkerhetsincidenter. En tidig rapportering av ett misstänksamt e-postmeddelande tillåter en organisation att omedelbart upptäcka en cyberattack av detta slag, utreda dess omfattning, samt sätta in lämpliga skyddsåtgärder. EY har därför även undersökt hur många mottagare av det förfalskade e-postmeddelandet att rapportera meddelandet. EY bedömer detta som ett viktigt område att granska, då det visar på hur medvetna medarbetarna inom kommunen är om hotet av phishing, samt dess kunskaper att agera i enlighet med kommunens riktlinjer när ett falskt e-postmeddelande upptäcks.

1.4.2 Genomförande

Övningen har utformats och genomförts av specialister inom IT- och informationssäkerhet från EY, tillsammans med utvalda representanter från Simrishamns kommun. De utvalda representanterna från kommunen har givits möjlighet att faktagranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekta fakta. Nedan följer en ingående beskrivning av respektive huvudmoment för att förbereda, utföra och analysera den simulerade attacken.

1.4.2.1 E-postmeddelande och landningssida

En simulerad phishing-attack bygger på att ett e-postmeddelande skickas ut till en utvald målgrupp. E-postmeddelandet kan vara utformat på olika sätt baserat på övningens syfte. E-postmeddelandet kan exempelvis innehålla en länk som leder vidare till en landningssida eller inkludera en länk som initierar en nerladdning av en fil. E-postmeddelanden som inkluderar en länk till en landningssida testar vanligtvis hur villiga medarbetarna är att dela med sig av användarinformation som inloggningsuppgifter eller att ladda ner okända filer.

För att bestämma hur e-postmeddelandet skulle utformas hölls inledningsvis möten tillsammans med kommunens representanter. Beslutet föll på att inkludera en länk i e-postmeddelande som hänvisade till en landningssida. Det aktuella meddelandet uppgavs vara skickat från kommunens Helpdesk, men skickades från en e-postadress med domänen ”simrishamnkommun.com”. En domän som inte tillhör Simrishamns kommun. I

epostmeddelandet uppmanades mottagaren att klicka på en länk för att öka utrymmet i sin inkorg då kvotgränsen påstås ha blivit överskiden. Genom att följa länken i epostmeddelandet landade besökaren på den förfalskade landningssidan där de ombads logga in med sitt Microsoft 365-konto (e-postadress och lösenord). Om en mottagare valde att fylla i sina användaruppgifter på landningssidan, skickades de vidare till ytterligare en landningssida som informerade mottagaren att de deltagit i en simulerad phishing-attack. Syftet med den informerande landningssidan är att skapa medvetenhet om informationssäkerhet i organisationen och informera om hotet av phishing. För e-postmeddelandet som skickades ut och de båda landningssidorna, se *bilaga 1* och *bilaga 2*.

1.4.2.2 Målgrupp och utskick

Målgruppen för en simulerad phishing-attack kan variera beroende på övningens syfte. E-postmeddelandet kan exempelvis vara riktat mot utvalda avdelningar eller bolag baserat på deras risknivå. E-postmeddelandet kan också skickas ut till samtliga anställda för att på så sätt skaffa sig en övergripande bild av kommunens motståndskraft och medarbetarnas medvetenhet.

I samråd med kommunens representanter beslutades att skicka ut e-postmeddelandet till samtliga medarbetare, med undantag för de kommunala bolagen, i syfte att få en övergripande bild av nivån för informationssäkerhet i praktiken i kommunen. Detta resulterade i att 2115 medarbetare inom kommunen deltog i övningen och att samtliga förvaltningar representerades i granskningen.

Innan det faktiska e-postmeddelandet skickades ut hölls ett testmöte där den simulerade attacken testades för att säkerställa att e-postmeddelandet gick igenom skalskyddet och fram till mottagarna. Den tekniska genomgången inkluderade behov av vitlistning, spamfilter och potentiell rate limiting[1]. Detta innebär att kommunens tekniska skydd kopplas bort, i syfte att på ett kostnadseffektivt sätt testa personalen och inte tekniken. Det bör noteras att inget tekniskt skydd fullständigt kan förhindra ett angrepp via phishing. EY startade simuleringen den 12 december 2022, då e-postmeddelandet skickades till samtlia mottagare. Simuleringen var aktiv i en veckas tid, fram till att den stängdes den 19 december 2022.

1.4.2.3 Rapportering

Att skydda sig mot hotet från en phishing-attack kan vara svårt och kräver en fungerande samverkan mellan flera olika faktorer. En viktig komponent är att effektiva rapporteringsvägar existerar och att medarbetarna är medvetna om hur dessa ska användas. Åtgärder bör vidtas skyndsamt då hotet är som störst under den initiala tiden efter att e-postmeddelandet mottagits. Det är också av stor vikt att personer som misstänker att de blivit utsatta för angrepp vidtar nödvändiga åtgärder för att ändra inloggningsuppgifter som en angripare kan ha fått tillgång till.

Inom Simrishamn kommun uppmanas medarbetare att inte klicka på länkar eller bilagor som ser konstiga ut eller där avsändaren är okänd. Vid misstanke om att skadlig kod eller

[1] För förklaring av begreppen, se definitioner i *bilaga 6*.

virus har inkommit via e-post uppmanas även medarbetarna att omedelbart kontakta IT-helpdesk. Denna information finns tillgänglig för samtliga medarbetare på kommunens intranät samt i en video uppladdad på kommunens egna Youtube-kanal. I informationssäkerhetspolicyn framgår det att samtliga medarbetare har ett ansvar att vara uppmärksamma på brister och incidenter rörande informationssäkerheten samt att rapportera dessa till närmsta chef och IT-helpdesk.

1.4.2.4 Enkät

Efter avslutad simulering distribuerades ett antal enkätfrågor via kommunen till mottagarna av e-postmeddelandet. Enkäten utformades av EY och syftet var att skapa en förståelse för motivationen och förmågan hos kommunens anställda att identifiera ett falskt e-postmeddelande. Därutöver var syftet även att undersöka om medarbetarna känner till befintliga riktlinjer, utbildningsmöjligheter och rapporteringsvägar. Se *bilaga 4* för enkäten som användes i samband med övningen.

1.4.2.5 Risknivåer och acceptansnivåer

För att tolka resultaten av en simulerad phishing-attack krävs en förståelse för potentiella risker av en fullbordad attack (risknivåer) och mottagarens relativa benägenhet att acceptera riskerna (acceptansnivåer). Risken för en fullbordad attack kan exempelvis vara mer omfattande för en större kommun då dessa besitter mer känslig information och större finansiell kraft. Det kan också vara skillnader inom en kommun där riskerna för vissa förvaltningar kan vara mindre än för andra beroende på typen av verksamhet. Se *tabell 1* för definitioner av risknivåer som EY har använt under genomförd granskning.

Tabell 1: Risknivåer för phishing-övning

Mycket hög risk	En mycket hög risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att omgående vidta åtgärder för att åtgärda svagheter i motståndskraften mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Hög risk	En hög risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att vidta åtgärder för att utvärdera och åtgärda svagheter i motståndskraften mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Medelhög risk	En medelhög risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att utvärdera och förbättra motståndskraften mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Låg risk	En låg risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att arbeta vidare med att kontinuerligt säkerställa en hög motståndskraft mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.

Innan en simulerad phishing-attack påbörjas är det viktigt att översätta de olika risknivåerna till specifika mätetal anpassade för den aktuella organisationen, vilket kallas för acceptansnivåer. För den simulerade övningen definierades acceptansnivåer i samråd mellan EY och kommunens representanter genom att omvandla risknivåerna till specifika procentandelar, se *bilaga 3*.

1.4.3 Tidsplan

Granskningen genomfördes från september 2022 till december 2022, se *tabell 2* nedan för granskningens tidsplan.

Tabell 2: Tidsplan

Förberedelser och planering	December 2022
Test och utskick	December – januari 2022
Rapportskrivning och intern kvalitetssäkring	Januari 2022
Justering och färdigställande av rapport	Februari 2022
Avrapportering och slutpresentation	Mars 2022

2. Analys

En phishing-attack kan genomföras på många olika sätt vilket kan påverka resultatet och eventuella konsekvenser av attacken. Beroende på vad en cyberkriminell aktör har för målsättning med en attack kan den vara mer eller mindre riktad till specifika personer eller avdelningar inom kommunen. Phishing-attackens utformning påverkar därmed resultatet och bör vägas in i analysen. I följande kapitel analyseras resultatet av den simulerade attack som EY gemensamt med kommunen utformat. Analysen presenteras i tre delar baserat på tre huvudområden: 2.1 Mottagare som klickat på länken i e-postmeddelandet, 2.2 Mottagare som uppgav användarinformation på landningssidan, och 2.3 Mottagares medvetenhet kring informationssäkerhet och phishing.

2.1 Mottagare som klickade på länken i e-postmeddelandet

I detta avsnitt presenteras andelen mottagare som klickade på länken i e-postmeddelandet. Simrishamns kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på kommunens omfattning och riskaptit. *Tabell 3* nedan beskriver de beslutade acceptansnivåerna för andelen mottagare som klickar på länken.

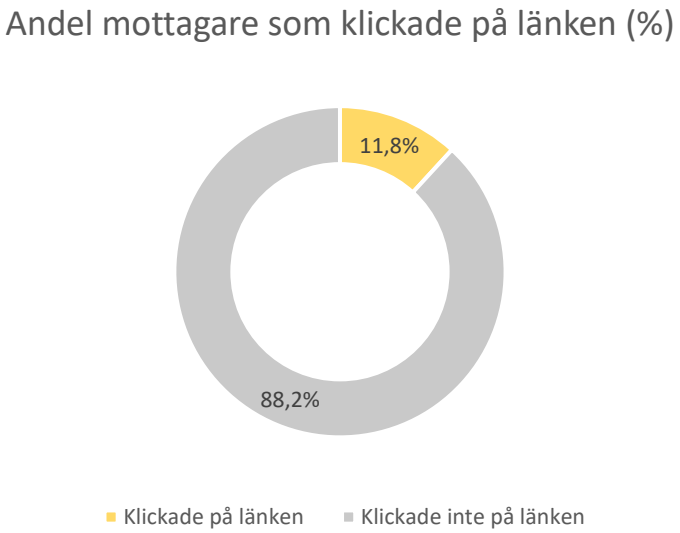
Resultatet av den simulerade attacken för kommunen som helhet visar att 11,8 procent av mottagarna klickade på den inbäddade länken i e-postmeddelandet. Resultatet av granskningen visar att enligt de definierade acceptansnivåerna löper Simrishamns kommun en hög risk att utsättas för phishing-attacker.

Tabell 3: Acceptansnivåer för andelen mottagare som klickar på länken

Riskanalys	Acceptansnivå (%)
Mycket hög risk	>15%
Hög risk	10-15%
Medel risk	5-10%
Låg risk	<5%

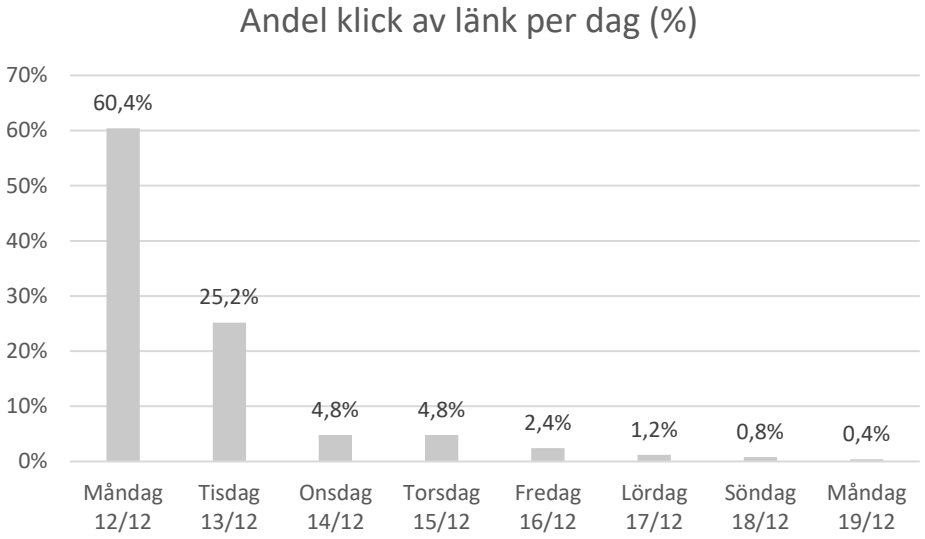
2.1.1 Resultat av simulering

E-postmeddelandet skickades till samtliga medarbetare inom kommunen. Det insamlade resultatet analyserade hur många mottagare som klickat på länken i det förfalskade meddelandet, dels för kommunen som helhet men även uppdelat på kommunens förvaltningar. Av 2115 mottagare klickade 250 mottagare på länken i e-postmeddelandet, vilket motsvarar 11,8 procent av mottagarna, se *figur 2* nedan. Det här resultatet innebär enligt acceptansnivåerna att Simrishamns kommun löper en hög risk för att utsättas för en fullbordad phishing-attack.



Figur 2: Fördelningen av andel mottagare som klickade på länken i e-postmeddelandet (%).

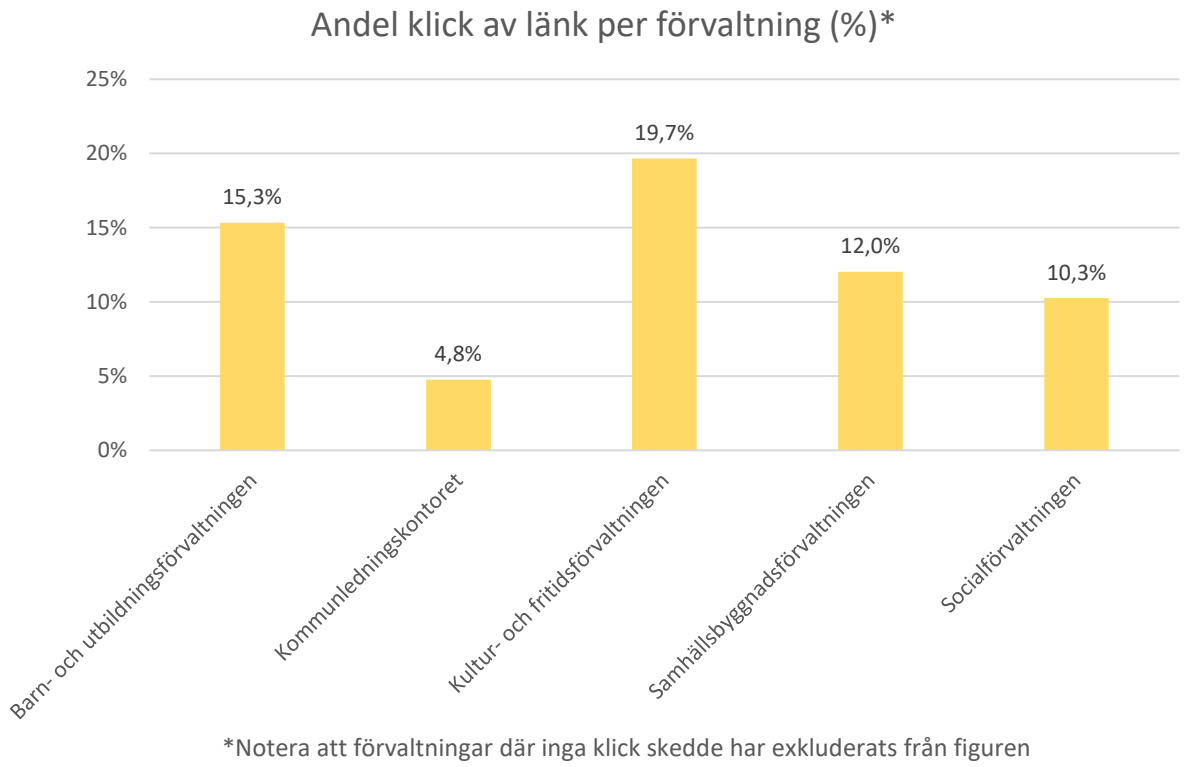
Simuleringen var aktiv under en veckas tid. I *figur 3* illustreras andelen klick på länken per dag, där det visualiseras att 60,4 procent av alla mottagare som klickade på länken i e-postmeddelandet gjorde det under simuleringens första dag. EY noterar att antalet klick på länken sjönk markant under de nästkommande dagarna och att ett fåtal klick skedde under helgen. Den här trenden är enligt EY förväntad i en simulerad attack då den påkallar omedelbara handlingar av mottagaren.



Figur 3: Andelen klick av länk i e-postmeddelandet under simuleringens aktiva period (%).

Figur 4 visar andelen klick på länken i e-postmeddelandet per förvaltning. EY noterar att andelen klick per förvaltning generellt är på en hög nivå i jämförelse med de på förhand bestämda acceptansnivåerna. EY noterar vidare att 19,7 procent av mottagarna inom kultur- och fritidsförvaltningen klickade på länken, vilken är den högsta andelen mottagare som klickat på länken inom medtagna förvaltningar. Vidare noterar EY att barn- och utbildningsförvaltningen också sticker ut med 15,3 procent av mottagare som klickat på

länken. Lägst andel mottagare som klickade på länken hade kommunledningskontoret. Enligt de bestämda acceptansnivåerna löper följande förvaltningar en medel till mycket hög risk att utsättas för en fullbordad phishing-attack.



Figur 4: Fördelning av mottagare som klickade på länken per förvaltning (%). Notera att andel mottagare som klickat på e-postmeddelandet baseras på antalet e-postmeddelanden som skickades till respektive förvaltning.

2.2 Mottagare som uppgav användarinformation på landningssida

I det här avsnittet presenteras andelen mottagare som efter att de klickat på länken i e-postmeddelandet även uppgav användarinformation i form av e-postadress och lösenord på landningssidan. Simrishamns kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på verksamhetens omfattning. *Tabell 4* beskriver de beslutade acceptansnivåerna för andelen mottagare som uppger användarinformation.

Resultatet av den simulerade attacken för kommunen som helhet visar att 4,6 procent av alla mottagare uppgav sin användarinformation på den förfalskade landningssidan. I relation till de på förhand definierade acceptansnivåerna indikerar resultatet på att Simrishamns kommun löper en hög risk att utsättas för en fullbordad phishing-attack. Notera att acceptansnivåerna för andelen mottagare som anger användarinformation på landningssidan generellt sett är lägre än för andelen mottagare som klickar på länken i e-postmeddelandet. Detta då EY anser att risken för en fullbordad phishing-attack är högre

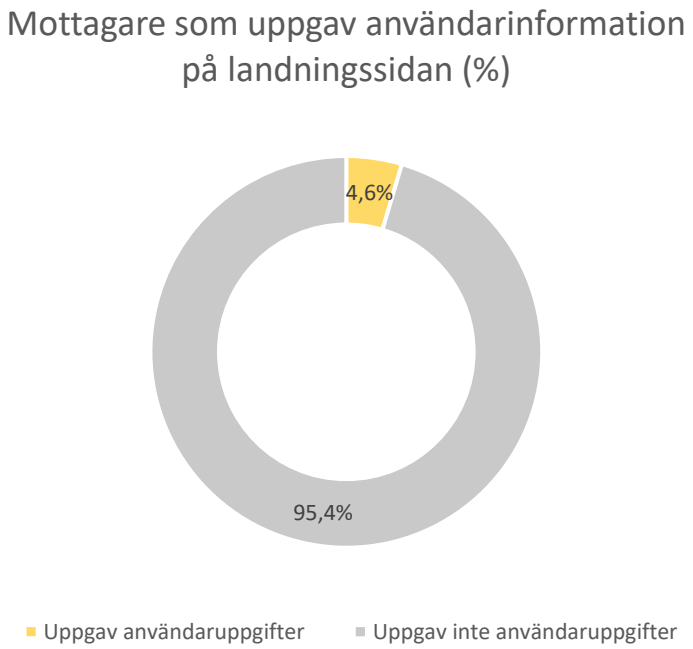
om en cyberangripare får tillgång till användardata och därmed potentiellt kommunens IT-miljöer.

Tabell 4: Acceptansnivåer för mottagare som uppger användarinformation på landningssidan

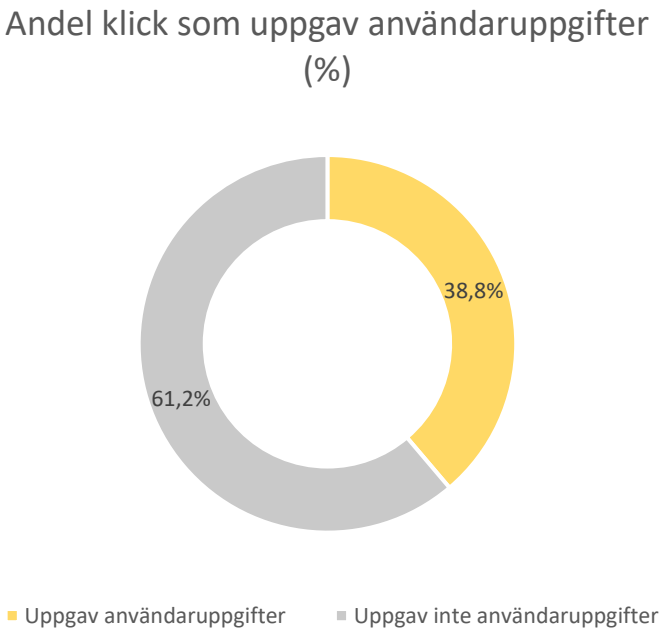
Riskanalys	Acceptansnivå (%)
Mycket hög risk	>6%
Hög risk	4-6%
Medel risk	2-4%
Låg risk	<2%

2.2.1 Resultat av simulering

Av det totala antalet mottagare (2115), klickade 97 medarbetare på länken samt uppgav sin användarinformation i form av användarnamn och lösenord på landningssidan. Det motsvarar 4,6 procent av alla mottagare, se *figur 5*. I jämförelse med acceptansnivåerna i *tabell 4*, löper därmed Simrishamns kommun som helhet en hög risk att utsättas för en fullbordad phishing-attack. Då 97 av de 250 medarbetare som klickade på länken även uppgav användarinformation, noterar EY att 38,8 procent av de som klickade på länken valde att uppge användarinformation medan resterande lämnade landningssidan (*figur 6*).

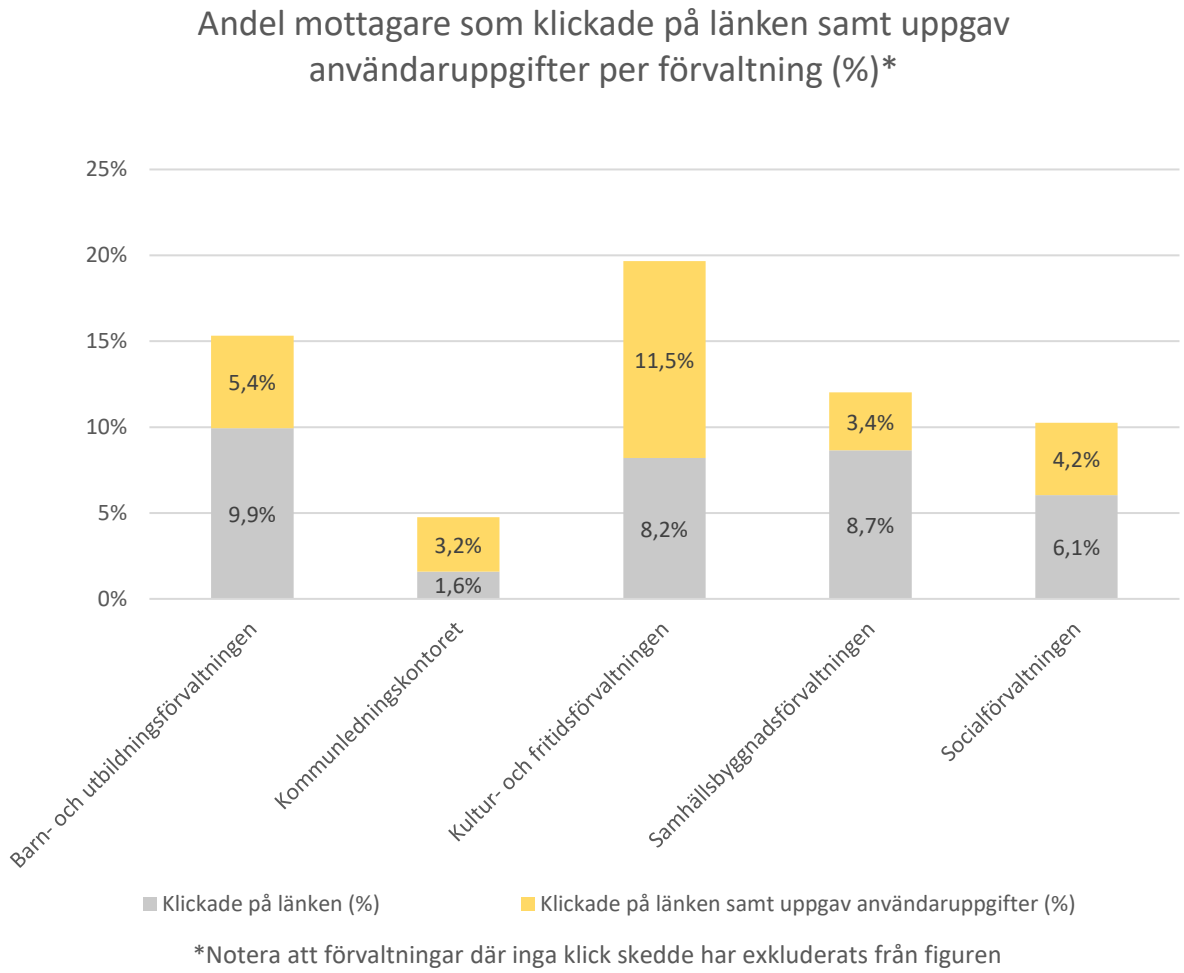


Figur 5: Fördelningen av andel mottagare som uppgav användarinformation på landningssidan (%). Resultatet inkluderar kommunen som helhet, dvs. inkluderat förvaltningarna.



Figur 6: Fördelningen av andel mottagare som uppgav användarinformation på landningssidan i relation till de mottagare som enbart klickade på länken. Resultatet inkluderar kommunen som helhet, dvs. inkluderat förvaltningarna.

Figur 7 visar andelen mottagare som klickade på länken i e-postmeddelandet i relation till andelen mottagare som utöver att klicka på länken även uppgav användarinformation på landningssidan. Som tidigare noterat var kultur- och fritidsförvaltningen den förvaltning där flest mottagare procentuellt klickade på länken. Samma förvaltning hade även högst andel mottagare som lämnade användarinformation på landningssidan (11,5 procent), detta följt av barn- och utbildningsförvaltningen och socialförvaltningen. Dessa hade ett resultat på 5,4 procent respektive 4,2 procent. Baserat på acceptansnivåerna noterar EY att verksamheternas risk varierar. Riskerna att utsättas för en fullbordad phishing-attack bedöms vara antingen medel hög, hög eller mycket hög. EY vill även betona att vid en verklig attack kan det räcka med att endast en användare uppger användarinformation för att aktören ska kunna ta sig in i och, i värsta fall, ta kontroll över kommunens IT-miljöer.



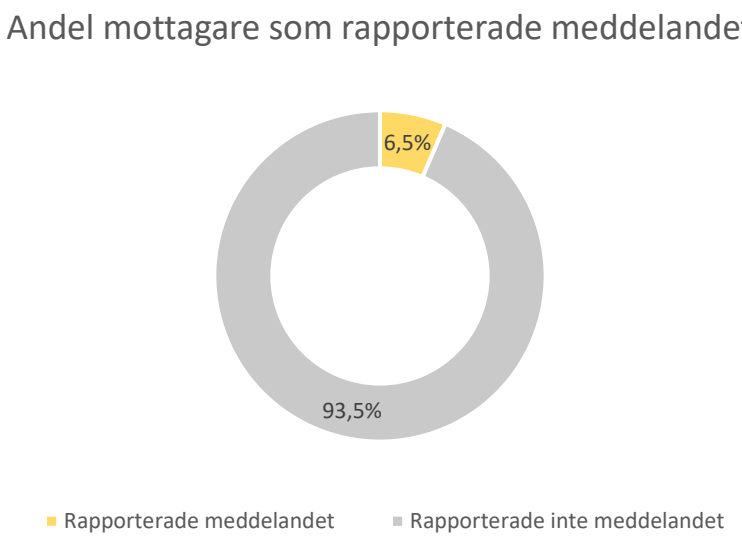
Figur 7: Andelen mottagare som klickade på länken i relation till mottagare som först klickade på länken och sedan lämnade användarinformation per förvaltning (%). Notera att andelen mottagare baseras på antalet e-postmeddelande som skickades till respektive förvaltning.

2.3 Mottagares medvetenhet kring informationssäkerhet och phishing

I detta avsnitt presenteras resultatet av andelen medarbetare som identifierade och misstänkte det förfalskade e-postmeddelandet och som valde att rapportera till kommunen. Avsnittet presenterar även resultatet av den enkät som distribuerades efter avslutad simulering. Syftet med enkäten var att skapa en övergripande förståelse för hur medvetna anställda i Simrishamns kommun är kring informationssäkerhet och phishing. Enkäten inkluderade frågor inom följande två områden: 1) e-postmeddelandet som användes i övningen och vanliga indikatorer på phishing, 2) säkerhetskulturen på kommunen i form av utbildning och medvetenhet, styrande dokument och rapportering av säkerhetsincidenter. Enkäten skickades ut till samtliga deltagare, varav 534 av dessa mottagare deltog i enkätundersökningen. Notera att i denna analys presenteras ett urval av enkätresultatet (se *bilaga 4* och *5* för den fullständiga enkäten).

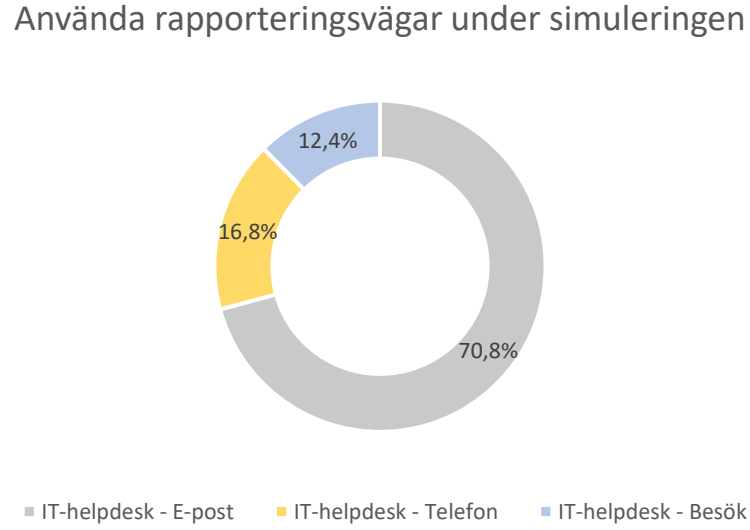
2.3.1 Rapportering

I Simrishamns kommun ska misstänksamma e-postmeddelanden rapporteras till kommunens IT-helpdesk. Totalt rapporterade 137 medarbetare e-postmeddelandet under pågående simulering, motsvarande 6,5 procent av alla mottagare, se *figur 8*.



Figur 8: Andel mottagare som rapporterade meddelandet

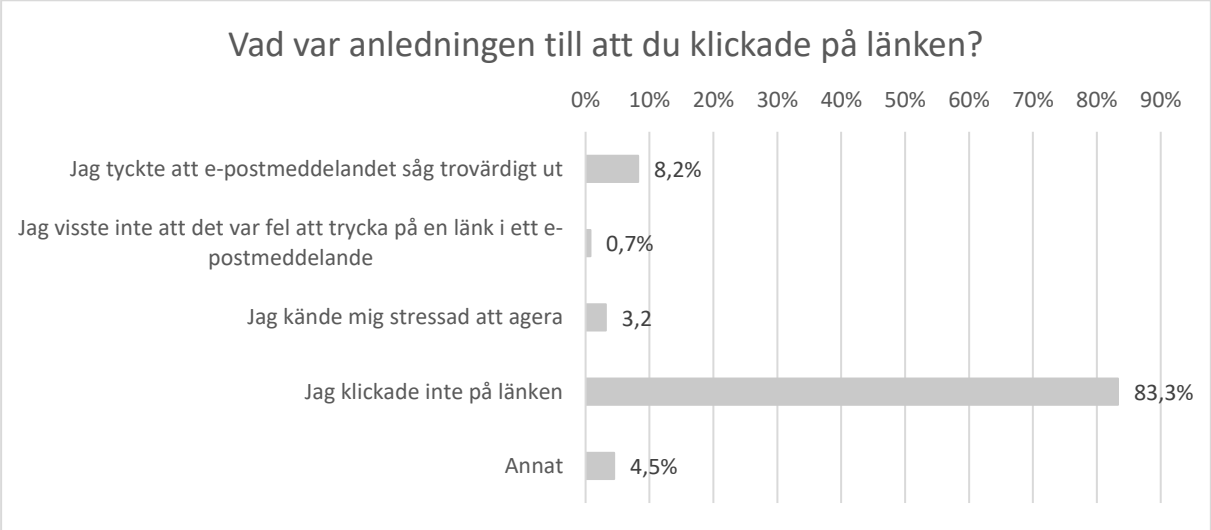
Rapporteringarna inkom till IT-helpdesk genom olika rapporteringsmetoder. *Figur 9* nedan visar att den mest frekvent använda rapporteringsmetoden till IT-helpdesk var via e-post, där 70,8 procent av medarbetarna som rapporterade e-postmeddelandet valde denna metod. Ytterligare valde 16,8 procent av de rapporterande medarbetarna att kontakta IT-helpdesk via telefon. Medarbetare valde även att fysiskt besöka IT-helpdesk för att rapportera e-postmeddelandet. Detta gjorde 12,4 procent av de rapporterande medarbetarna.



Figur 9: Fördelning av använda rapporteringsvägar under pågående simulering (%).

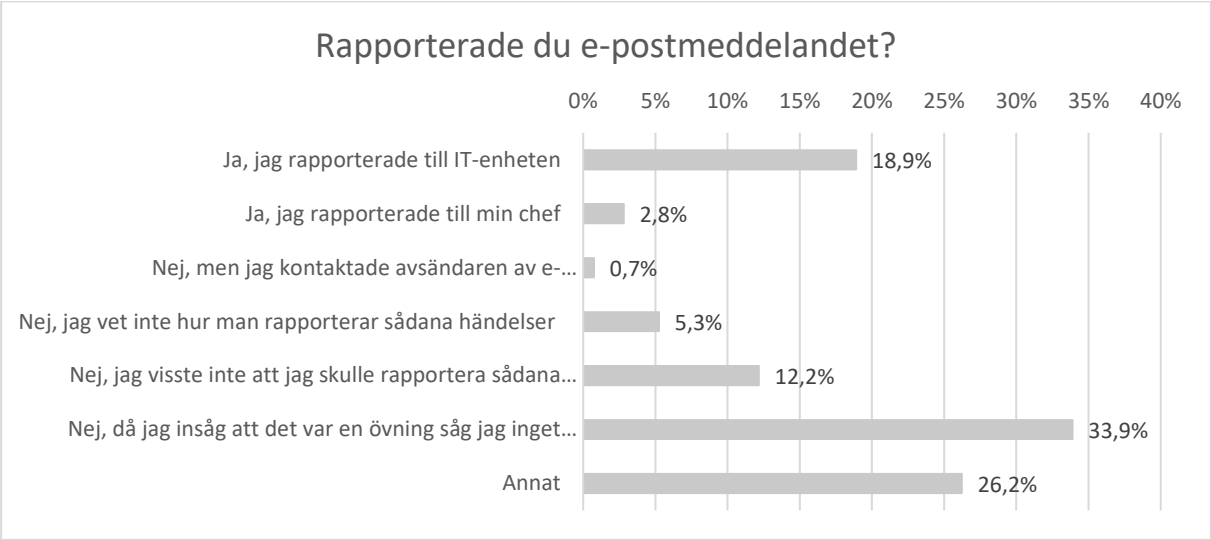
2.3.2 Resultat av enkät

Medarbetares förmåga att identifiera ett falskt e-postmeddelande är av stor vikt för att Simrishamns kommun ska kunna minimera riskerna för en fullbordad phishing-attack. *Figur 10* visar olika anledningar till att mottagarna av e-postmeddelandet klickade på den inbäddade länken i e-postmeddelandet. Av de som uppgav att de klickade på länken svarade flest mottagare att de tyckte att e-postmeddelandet såg trovärdigt ut, motsvarande 8,2 procent av alla svarande. 3,2 procent av deltagarna uppgav att de klickade på länken för att de upplevde stress att agera i enlighet med e-postmeddelandets uppmaning. Samtidigt uppgav 0,7 procent av mottagarna andra anledningar till att de klickade på länken. Det handlade bland annat om medarbetare som var stressade eller upplevt liknande uppmaningar till agerande förr. 83,3 procent av de svarande klickade inte på länken.



Figur 10: Resultat av enkätfråga om länken i e-postmeddelandet (%).

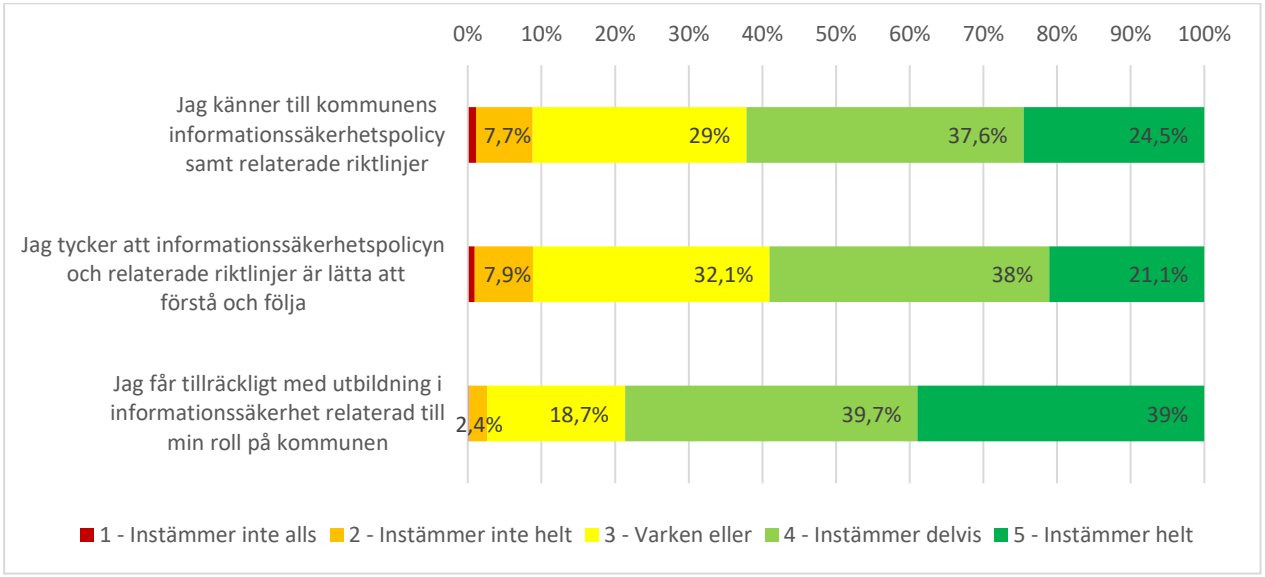
Resultaten visade även att majoriteten av inrapporteringarna skedde till IT-enheten, då 18,9 procent av de svarande som rapporterade händelsen kontaktade IT-enheten. Samtidigt var 12,2 procent av de svarande omedvetna om att händelser som denna ska rapporteras, och 5,2 procent uppgav att de var omedvetna om hur händelser som denna ska rapporteras. 26,6 procent av de svarande uppgav "annat", vilket främst bestod av anledningar såsom tidsbrist och att kollegor redan rapporterat händelsen.



Figur 11: Resultat av enkätfråga om rapportering av e-postmeddelandet (%).

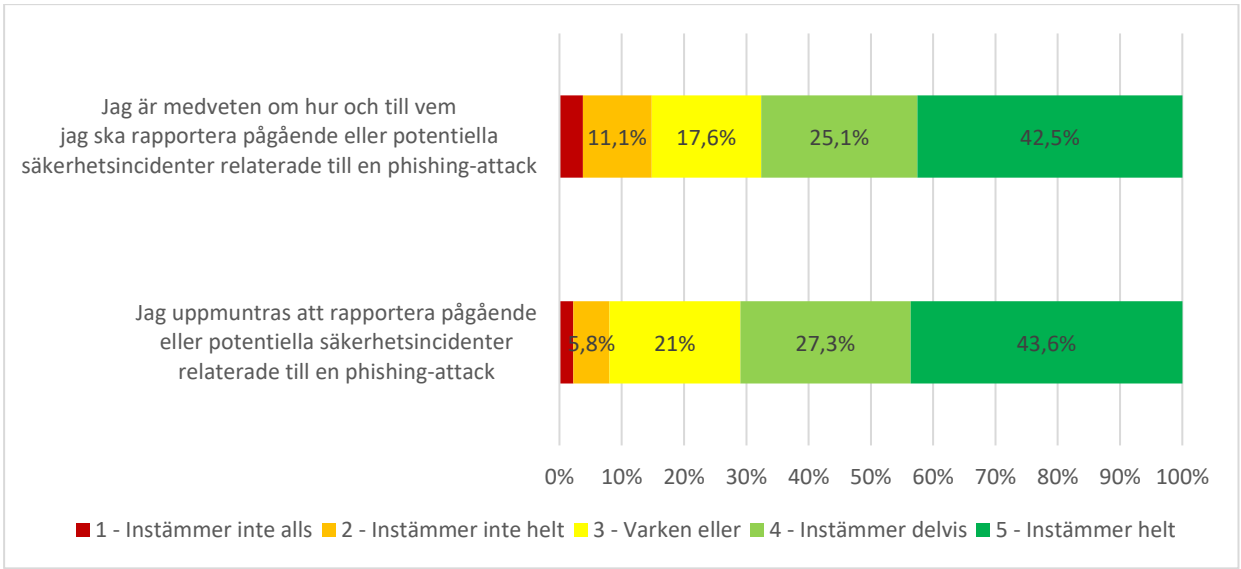
Enkätresultatet visade att 24,5 procent av deltagarna instämmer helt till påståendet att de känner till kommunens nuvarande informationssäkerhetspolicy och relaterade riktlinjer. Den största andelen av deltagarna anger "Instämmer delvis" till samma påstående (37,6 procent), samtidigt som 1,1 procent av deltagarna inte alls instämmer att de känner till kommunens informationssäkerhetspolicy. När det kommer till huruvida informationssäkerhetspolicyn och relaterade riktlinjer är lätta att förstå och följa uppger 31,1 procent av enkätdeltagarna varken eller. 38 procent av enkätdeltagarna väljer svarsalternativet "Instämmer delvis", 21,1 procent väljer svarsalternativet "Instämmer helt", samtidigt som 0,9 procent av enkätdeltagarna väljer alternativet "Instämmer inte alls".

Närmare 39 procent av enkätdeltagarna uppgav "Instämmer helt" eller "Instämmer delvis" på frågan gällande tillräckligheten av utbildning inom informationssäkerhet relaterat till deras tjänst på kommunen. 18,7 procent av deltagarna instämmer till svarsalternativet "varken eller", medan 2,4 procent respektive 0,2 procent av deltagarna inte helt instämmer eller inte alls anser sig få tillräcklig utbildning inom området. Se *figur 12* för det fullständiga resultatet för dessa påståenden.



Figur 12: Resultat av påståenden om styrande dokument och utbildning inom informationssäkerhet på kommunen (%).

Enkätresultatet indikerar att det råder en viss oklarhet hos enkätdeltagarna kring kommunens rapporteringsrutiner vid säkerhetsincidenter relaterade till en phishing-attack. EY noterar att 11,1 procent av deltagarna anser att de inte helt vet hur de ska gå tillväga och vem de ska kontakta för att rapportera en pågående phishing-attack. Samtidigt uppger 42,5 procent och 25,1 procent av enkätdeltagarna att de känner till hur och till vem de ska rapportera en pågående phishing-attack respektive att de delvis vet, medan 17,6 procent svarar "varken eller". I relation till detta uppgav 5,8 procent av deltagarna att de inte helt instämmer till påståendet att de uppmuntras av kommunen att rapportera potentiella eller pågående säkerhetsincidenter. Samtidigt instämmer 43,6 procent av deltagarna helt till detta påstående. 21 procent av deltagarna svarar "varken eller" och 27,3% av deltagarna svarar "Instämmer delvis". Se *figur 13* för det fullständiga resultatet för dessa påståenden.



Figur 13: Resultat av påståenden om phishing-attacker och rapportering (%).

3. Övergripande rekommendationer

Baserat på den genomförda analysen bedömer EY att Simrishamns kommun ligger på en nivå under det man bör förvänta sig av jämförbara organisationer inom den kommunala sektorn. Bedömningen baseras på den typ av verksamhet som bedrivs och på känslighetsgraden av den information, exempelvis personuppgifter, som behandlas i den dagliga verksamheten. Således rekommenderar EY att man inom kommunen vidtar åtgärder för att stärka graden av utbildning och medvetenhet hos medarbetarna och därmed stärker motståndskraften mot phishing-attacker. Detta för att undvika förluster av känslig information, negativt rykte eller andra betydande konsekvenser. I följande avsnitt presenterar EY fyra övergripande rekommendationer som bedöms vara relevanta för Simrishamns kommun.

3.1 Tydliggör och informera om rutiner för rapportering av misstänkta e-postmeddelanden

En organisation kan minska effekterna av en pågående cyberattack genom att underlätta identifiering av attacken, förhindra spridningen och effektivt stoppa den. En förutsättning för att minimera konsekvenserna av en attack är att effektiva rapporteringsvägar existerar och att medarbetare är medvetna om hur och när dessa ska användas. Rapportering av ett misstänksamt e-postmeddelande kan möjliggöra att hotet identifieras och att skyddsåtgärder kan vidtas inom skälig tid.

Under de inledande mötena med kommunens kontaktpersoner informerades EY att IT-Helpdesk omedelbart ska kontaktas vid en incident. Denna riktlinje finns dokumenterad i rutinen för incidentrapportering, samt på kommunens intranät. EY noterade att uppmanad rapporteringsmetod varierade mellan de olika dokumentationerna. Resultatet av granskningen indikerar att medarbetarnas medvetenet av rapporteringsvägar för säkerhetsincidenter relaterade till phishing varierar. 12,2 procent av enkätdeltagarna uppgav att de inte visste att de skulle rapportera sådanna händelser som den som simulerades. Samtidigt uppgav 5,3 procent att de inte vet hur sådana händelser ska rapporteras. Granskningen visade även att endast 6,5 procent av medarbetarna rapporterade händelsen till IT-helpdesk.

EY rekommenderar att man med fördel bör specificera önskade rapporteringsmetoder för att kontakta IT-helpdesk. Detta eftersom det vid en pågående säkerhetsincident likt phishing är avgörande att kommunens incidenthanteringspersonal snabbt kan bilda sig en förståelse av vad som har inträffat. EY rekommenderar således kommunstyrelsen att konkret informera om hur medarbetare ska kontakta IT-helpdesk.

Utöver detta rekommenderar EY att Simrishamn kommun arbetar vidare med att kommunicera vikten av att rapportera eventuella säkerhetsincidenter. Kommunikationen bör inkludera tydliga förväntningar och kravställningar på rapportering hos samtliga medarbetare då man misstänker att man blivit utsatt för en phishing-attack. Detta för att öka sannolikheten att fler medarbetare vet om att en säkerhetsincident relaterat till phishing ska rapporteras, samt väljer att rapportera.

3.2 Teoretiska och praktiska utbildningar avseende identifiering av phishing

I takt med att mängden cyberattacker mot organisationer har ökat de senaste åren har EY noterat en markant ökning av phishing-attacker. Medarbetares medvetenhet och kunskap om informationssäkerhet blir således allt viktigare för att säkerställa ett adekvat skydd av informationen hos en organisation. Vidare ställs krav på att uppfylla lagar och regleringar om informationssäkerhet och dataskydd. En phishing-attack kan leda till allvarliga konsekvenser för kommunen, dels genom att utvinna känslig och konfidentiell information, dels genom att implementera skadlig kod på mottagarens enhet.

Under de inledande mötena med kommunens kontaktpersoner informerades EY att Simrishamn kommun sedan maj 2022 genomfört utbildningsinsatser inom informationssäkerhet för samtliga medarbetare. Den simulerade övningen visade att 11,8 procent av samtliga mottagare klickade på länken i e-postmeddelandet och att 4,6 procent av samtliga mottagare uppgav sin användarinformation på landningssidan. Baserat på resultatet och de satta acceptansnivåerna löper Simrishamn kommun en hög risk att utsättas för en fullbordad phishing-attack. Därtill uppgav 8,2 procent av enkätdeltagarna att de tyckte att e-postmeddelandet som användes för den simulerade attacken såg trovärdig ut. Med anledning av detta rekommenderar EY att nuvarande utbildninginsatser inom informationssäkerhet och phishing inkluderar ett fokus på hur falska e-postmeddelanden, domäner och hemsidor kan identifieras. Detta för att öka sannolikheten att phishing-attacker upptäcks i tid och för att minska risken att medarbetaren inte agerar mot phishing-attacken.

3.3 Målgruppsanpassa utbildningsinsatser

Utbildningar inom informationssäkerhet och phishing syftar till att förbättra medarbetares medvetenhet och kunskap inom området, och därtill stärka kommunens skydd mot cyberattacker. Under de inledande mötena med kommunens kontaktpersoner informerades EY att de utbildningsinsatser som införts inom informationssäkerhet på Simrishamn kommun tillgängligjorts för samtliga medarbetare. Samtidigt upplever kommunen ett lågt deltagande, där färre än hälften av kommunens medarbetare deltagit i utbildningen.

Resultatet av simuleringen visar vilka delar av kommunen som löper störst risk att inte agera på en phishing-attack i enlighet med kommunens riktlinjer, och där riktade utbildningsinsatser kan behövas. EY noterar även att kommunen består av medarbetare inom olika riskgrupper, med anledning av respektive verksamhets syfte och känslighetsgraden på informationen som hanteras. EY rekommenderar att kommunstyrelsen säkerställer att nuvarande utbildningssatser utvecklas och att man inför riktade och målgruppsanpassade utbildningar som ger medarbetare rätt kunskap att stå emot hot relaterade till informationssäkerhet. Detta för att säkerställa att medarbetare som är verksamma i de delar av kommunen där risken att utsättas för en fullbordad phishing-attack är störst utbildas inom informationssäkerhetsincidenter.

Under de inledande mötena med kommunens kontaktpersoner informerades EY att två uppföljningstillfällen i form av praktisk tillämpning har skett för samtliga medarbetare. EY rekommenderar att kommunstyrelsen säkerställer att utbildningar följs upp med regelbundna tester av säkerhetsmedvetenhet och kunskap inom phishing hos medarbetarna. Detta för att kontrollera effekten av genomförda utbildningsinsatser och för att fortsätta sprida kunskapen inom kommunen. Tillvägagångssätt som kan tillmpas inom kommunen är förslagsvis interaktiva utbildningsmaterial och nätbaserade simuleringar.

3.4 Inolvera riktlinjer för informationssäkerhet och phishing vid rekrytering

Enligt EY:s ramverk för hur en organisation arbetar med informationssäkerhet styrs en organisations motståndskraft av dess medarbetares motivation och förmågor. Motivation och förmågor formas av olika organisatoriska åtgärder såsom styrning, organisation, kommunikation, utbildning och styrdokument. För att erhålla en god motståndskraft mot cyberattacker krävs således ett övergripande, strukturerat och planlagt arbete med informationssäkerhet.

37,6 procent av medarbetarna uppgav i enkäten att de delvis känner till kommunens informationssäkerhetspolicy och relaterade riktlinjer, samtidigt som 29 procent av enkätdeltagarna svarade varken eller. Enkäten påvisade även att det finns viss förbättringspotential gällande hur väl medarbetarna känner sig insatta och förstår gällande riktlinjer och styrdokument på området. Resultatet av simuleringen tyder på att medarbetarnas kännedom om hur kommunen arbetar med informationssäkerhet och phishing är relativt låg, vilket avspeglar sig i andelen medarbetare som klickade på den inbäddade länken samt andelen medarbetare som även uppgav sin användarinformation på landningssidan.

Under de inledande mötena med kontakpersoner från kommunen informerades EY att styrdokument och dokumenterade riktlinjer finns tillgängliga för medarbetarna på kommunens intranät. Därtill informerades EY att berörda dokument och riktlinjer inte enligt utsatt process introduceras för medarbetare i samband med anställning. För att stärka arbetet med informationssäkerhet och phishing inom Simrishamn kommun rekommenderar EY att styrdokument och riktlinjer tydligt introduceras och kommuniceras till medarbetare i samband med anställning. Detta för att öka sannolikheten att fler medarbetare inom kommunen har kännedom om och har tagit del av relevanta styrdokument och riktlinjer för säkerhetsincidenter.

4. Revisionsfrågor

Granskningen har utgått från tre revisionsfrågor. Hur väl Simrishamns kommun svarar upp mot dessa revisionsfrågor beskrivs nedan.

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvarad delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Revisionsfråga	Svar	
▸ Hanterar Simrishamns kommuns personal hotet från attacker genom falska email, så kallad phishing (nätfiske), på ett ändamålsenligt sätt?	Baserat på den genomförda granskningen bedömer EY att Simrishamns kommun bör arbeta för att förbättra sin motståndskraft mot phishing. Bedömningen baseras på resultatet av simuleringen där 11,8 procent av medarbetarna klickade på länken. Resultatet tyder på att kommunen löper en hög risk att utsättas för en fullbordad phishing-attack. Därutöver uppgav 4,6 procent av medarbetarna användarinformation. EY vill betona att det räcker med att endast *en användare* uppger användarnamn och lösenord för att en angripare ska komma åt kommunens IT-miljöer. Slutsatsen är att Simrishamns kommun inte hanterar hotet från phishing-attacker på ett ändamålsenligt sätt.	
▸ Har Simrishamns kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av den testade personalen under den simulerade attacken?	Simrishamns kommuns incidenthanteringsprocess är dokumenterad och finns tillgänglig för samtliga medarbetare på kommunens intranät. Kommunens medarbetare uppmanas att kontakta IT-helpdesk via valfri metod vid ett misstänkt e-postmeddelande. Då uppmanad rapporteringsmetod inte är enhetlig mellan samtliga dokument, kan otydligheter leda till att få följer incidenthanteringsprocessen. Därutöver visade simuleringen att endast 6,5 procent av medarbetarna rapporterade ärendet. Detta tyder på en otydlighet bland medarbetarna gällande incidentrapportering, vilket kan leda till ineffektiv hantering av incidenter.	

	Därmed bedömer EY att kommunen inte har en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av medarbetarna under den simulerade attacken.	
► Är riktlinjer för hantering och rapportering av falska email och andra incidenter kända hos personalen?	I Simrishamns kommun finns dokumenterade riktlinjer för hur medarbetarna ska hantera ett förmodat falskt e-postmeddelande vid en phishing-attack. Dessa riktlinjer finns tillgängliga för samtliga medarbetare. Granskningen visar att medarbetare i viss utsträckning uppger att riktlinjerna är svåra att förstå och 12,2 procent av medarbetarna uppgav att de inte visste att en sådan incident som simulerades ska rapporteras. Detta försvårar för kommunen att ha en god beredskap vid en pågående phishing-attack. Således bedömer EY att kommunen delvis har kommunicerat instruktioner och riktlinjer för informationssäkerhet till medarbetarna på ett tillfredsställande sätt.	

5. Slutsatser

Den här granskningen syftade till att bedöma om kommunstyrelsen har säkerställt en tillräcklig intern kontroll avseende kommunens arbete med IT- och informationssäkerhet inom området falska e-postmeddelanden. Genom en simulerad phishing-attack har EY undersökt utbildning och medvetenhet hos medarbetarna.

Den genomförda granskningen svarar på följande revisionsfrågor:

- Hanterar Simrishamns kommuns medarbetare hotet från attacker genom falska email, så kallad phishing (nätfiske), på ett ändamålsenligt sätt?
- Har Simrishamns kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av den testade personalen under den simulerade attacken?
- Är riktlinjer för hantering och rapportering av falska email och andra incidenter kända hos personalen?

Resultatet visar att det finns ett behov av att förbättra utbildning och medvetenhet inom IT- och informationssäkerhet och phishing, då en stor andel medarbetare inte har tillräcklig kunskap inom området för att kunna identifiera ett falskt e-postmeddelande. Vidare visade resultatet av enkäten på att en stor andel av medarbetarna inte är medvetna om kommunens riktlinjer för informationssäkerhet, eller hur och när de ska rapportera en säkerhetsincident relaterad till e-postmeddelanden. Kommunstyrelsen rekommenderas därför att vidta åtgärder för att informera och tydliggöra relaterade styrdokument och riktlinjer, konkretisera rapporteringsvägar, och stärka utbildning och medvetenhet hos medarbetarna. En förbättrad motståndskraft mot phishing kan bidra till att förluster av känslig information, negativt rykte eller andra betydande konsekvenser minskar.

Baserat på resultatet från granskningen har EY valt att presentera följande fyra övergripande rekommendationer till kommunstyrelsen:

- Tydliggör och informera om rutiner för rapportering av misstänkta e-postmeddelanden.
- Genomför teoretiska och praktiska utbildningar avseende identifiering av phishing.
- Målgruppsanpassa utbildningsinsatser.
- Utbilda nyanställda i riktlinjer för informationssäkerhet och phishing.

Stockholm, 2023-02-22

Helena Törnqvist

Partner, EY

Bilaga 1: E-postmeddelande

E-postmeddelande

Varning: Kvotgräns överskriden

Helpdesk <Helpdesk@simrishamnkommun.com>
To

Reply | Reply All | Forward | ...
tor 2022-12-08 10:09

This sender Helpdesk@simrishamnkommun.com is from outside your organization.
Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
We converted this message into plain text format.

You don't often get email from helpdesk@simrishamnkommun.com. Learn why this is important <https://aka.ms/LearnAboutSenderIdentification>

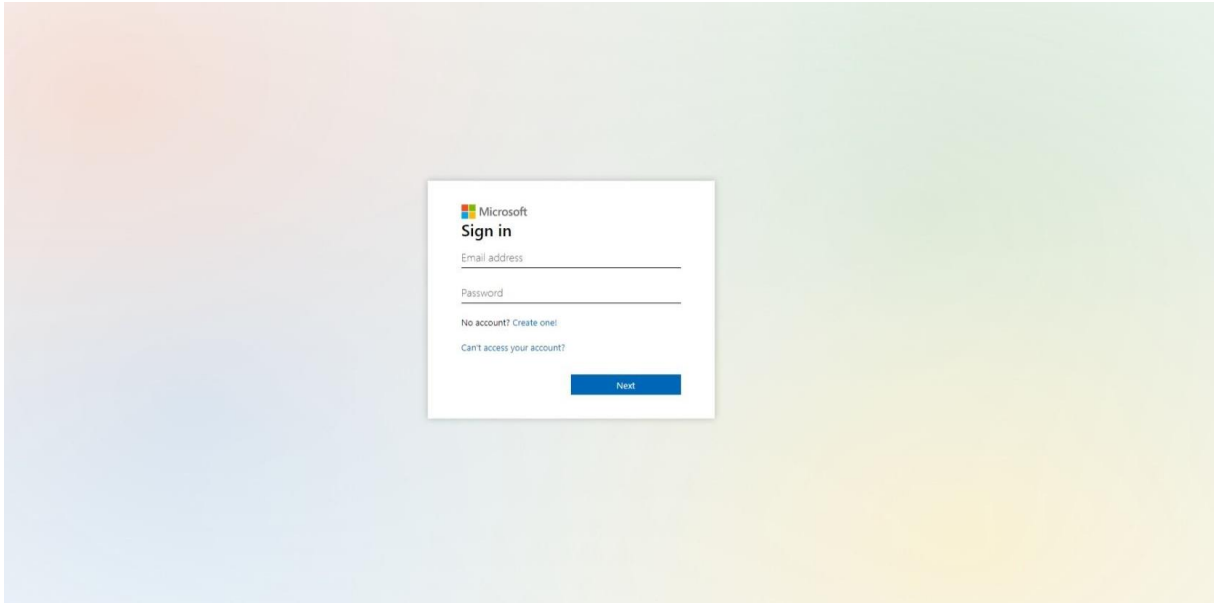
Hej,

Detta mail är en automatiserad varning för att notifiera dig att din inkorg överskridit sin kvotgräns. Du kommer inte att kunna skicka eller ta emot nya e-postmeddelanden förrän du har ökat utrymmet i din inkorg. Vänligen klicka här <https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsimrishamnkommun.com%2F%3Frid%3DO7Kdw4U&data=05%7C01%7Cshirin.jamshir%40se.ey.com%7C797171e5282a4d238fd508dad8fbc581%7C5b973f9977df4bebb27daa0c70b8482c%7C0%7C0%7C638060874018601806%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000%7C%7C%7C&sdata=Fq4ilCtz6jmutMMv1vKrchO6IFC4z8PXGg6mqqzzmiU%3D&reserved=0> för att lägga till mer utrymme till ditt konto.

Med vänliga hälsningar,
Helpdesk

Bilaga 2: Landningssida

Landningssida 1



Landningssida 2

OBS! Detta e-postmeddelande var nätfiske.

Det här är en simulering för att stärka Simrishamns motståndskraft mot cyberattacker genom phishing (svenska: nätfiske)

Denna övning utfördes i samarbete med EY som en del av kommunens arbete med informationssäkerhet. Vi hoppas med den här övningen utveckla medvetenheten om potentiella cyberattacker hos oss på kommunen.

Bedrägerier i form av social manipulation så som phishing är ett växande problem i samhället och ett förfalskat e-postmeddelande kan vara svårt att upptäcka. Vänligen se tips nedan på hur du i framtiden lyckas känna igen denna typ av e-postmeddelanden. Både på arbetsplatsen och i privata sammanhang.

Den användarinformation du har angett är anonymiserad och kommer att raderas. Det är endast aggregerad statistik som kommer samlas in.

Vi vill bedöma anställdas grad av försiktighet och medvetenhet om phishing och uppskattar därför om du inte diskuterar detta mejl med kollegor eller informerar dem om övningen.

Stanna upp, se efter, tänk till!

Finns det något i e-postmeddelandet som var ovanligt? Bedragare utnyttjar ofta stressiga situationer för att få oss att agera hastigt. Var särskilt kritisk till e-postmeddelanden som uppmanar dig att kringgå vanliga procedurer och/eller agera snabbt. Är det troligt att du skulle få den här typen av e-postmeddelande utan någon tidigare information från din arbetsgivare?

Om du misstänker att du har utsatts för en phishing-attack, kontakta genast Helpdesk hos kommunen.

1. Kontrollera avsändare

Om du misstänker att ett e-postmeddelande inte är äkta, tänk på att vara kritisk till innehållet och leta efter saker som inte stämmer. Domänen simrishamnkommun.com, från vilken e-postmeddelandet skickades, är inte en domän som Simrishamn använder utan en så kallad bluffdomän. Dessa är gjorda så att man vid första anblick inte ska misstänka att någonting är fel.

2. Kontrollera länkar

Klicka aldrig på länkar inbäddade i e-postmeddelande om du misstänker att någonting inte stämmer, eller om du inte förväntar dig att få liknande e-postmeddelanden.

3. Kontrollera språket

Håll utkik efter stavfel. Seriösa e-postmeddelanden innehåller oftast inte stavfel och brukar inte vara skrivna på dålig svenska. Men det är viktigt att förstå att cyberkriminella även kan använda sig av mer sofistikerade metoder. Notera att dessa typer av e-postmeddelanden även kan vara välformulerade, som i den här simulerade övningen.

Bilaga 3: Acceptansnivåer

	Mycket hög risk	Hög risk	Medel risk	Låg risk
Andel mottagare som klickar på länken i e-postmeddelandet	>15%	10-15%	5-10%	<5%
Andel mottagare som uppger användarinformation på landningssidan	>6%	4-6%	2-4%	<2%

Bilaga 4: Enkätfrågor

Frågor om e-postmeddelandet

1. Vad var anledningen till att du klickade på länken?
    - Jag tycker att e-postmeddelandet såg trovärdigt ut
    - Jag visste inte att det var fel att trycka på en länk i ett e-postmeddelande
    - Jag kände mig stressad att agera
    - Jag klickade inte på länken
    - Annat

2. När insåg du att det här e-postmeddelandet var "phishing"?
    - När jag såg e-postmeddelandet
    - När jag klickat på länken och skickades till landningssidan
    - När jag hade lämnat mina uppgifter och såg informationen om övningen
    - När jag blev varnad om att e-postmeddelandet var falskt, exempelvis från en kollega eller kommunen
    - Annat

3. Rapporterade du e-postmeddelandet?
    - Ja, jag rapporterade till IT-avdelningen
    - Ja, jag rapporterade via en annan rapporteringskanal
    - Nej, men jag kontaktade avsändaren av e-postmeddelandet
    - Nej, jag vet inte hur man rapporterar sådana händelser
    - Nej, jag visste inte att jag skulle rapportera sådana incidenter
    - Nej, då jag insåg att det var en övning såg jag inget behov av att rapportera det
    - Annat

Frågor om säkerhetskulturen

Frågorna om säkerhetskultur delas upp i tre underområden: 1) Utbildning och medvetenhet, 2) Policy och riktlinjer, och 3) Rapportering. Följande frågor besvaras på en skala enligt nedan:

1. Instämmer helt
2.
3.
4.
5. Instämmer inte alls.

Utbildning och medvetenhet

- Jag får tillräcklig utbildning i informationssäkerhet relaterad till min roll på kommunen
- Jag får kontinuerlig, relevant och tillräcklig information om informationssäkerhet från kommunen
- Jag vet vad en phishing-attack är och hur man ska reagera på sådana attacker

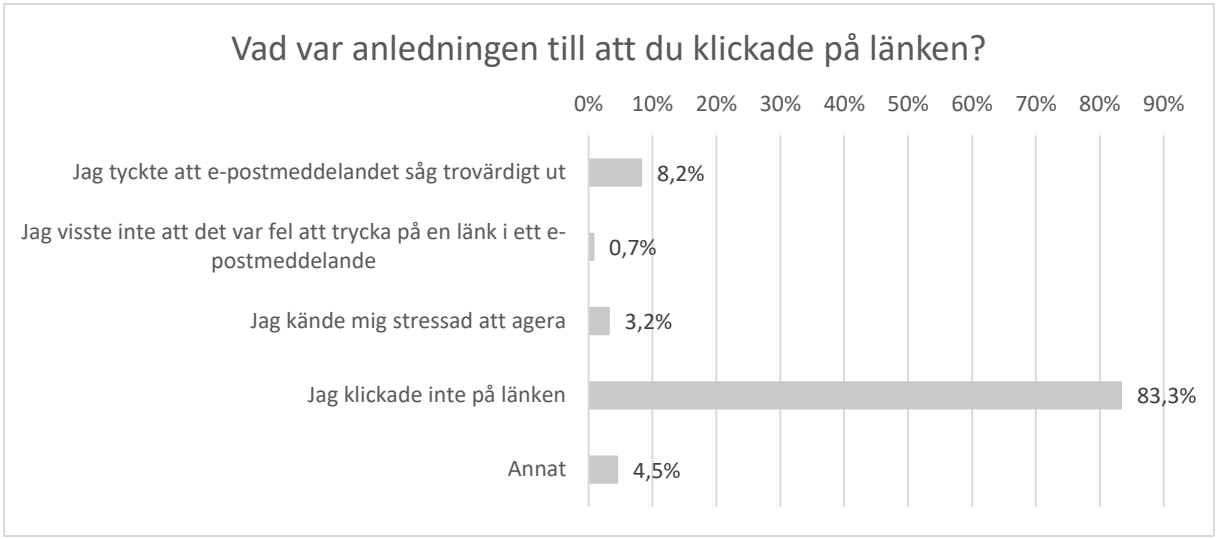
Policy och riktlinjer

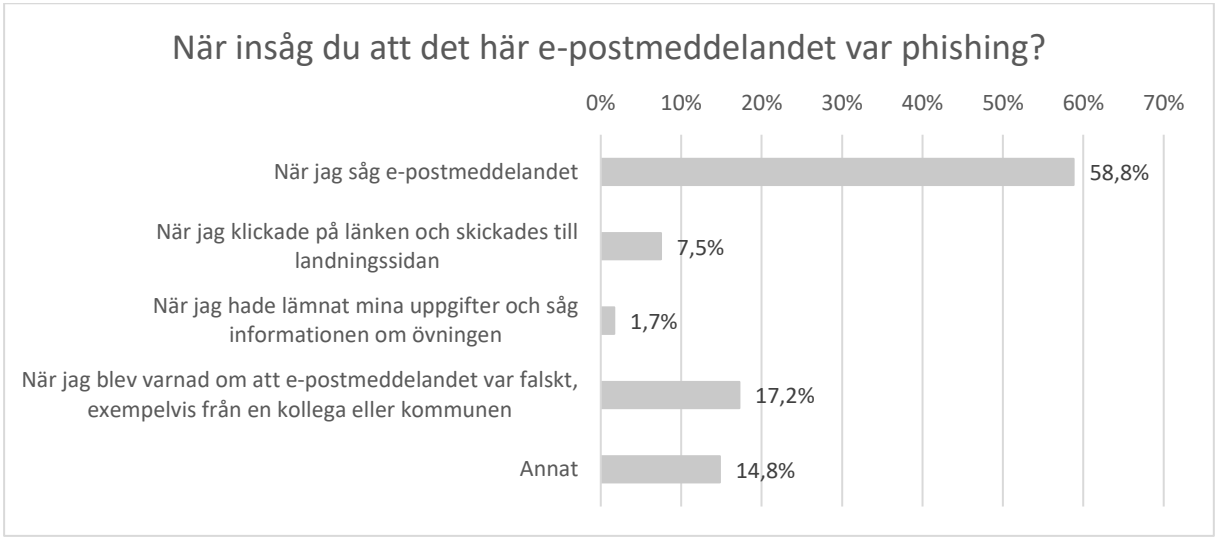
- Jag känner till kommunens informationssäkerhetspolicy samt relaterade riktlinjer
- Jag tycker att informationssäkerhetspolicyn och relaterade riktlinjer är lätta att förstå och följa
- Jag är medveten om de potentiella hot och negativa konsekvenser som kan uppstå av att inte efterleva kommunens policyer och riktlinjer kring informationssäkerhet.

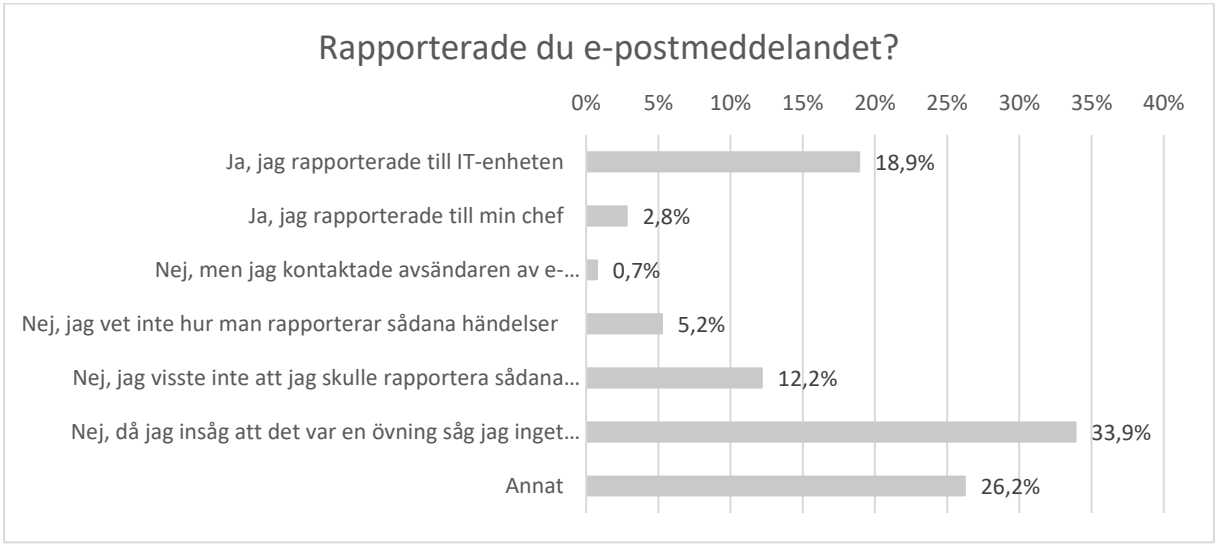
Rapportering

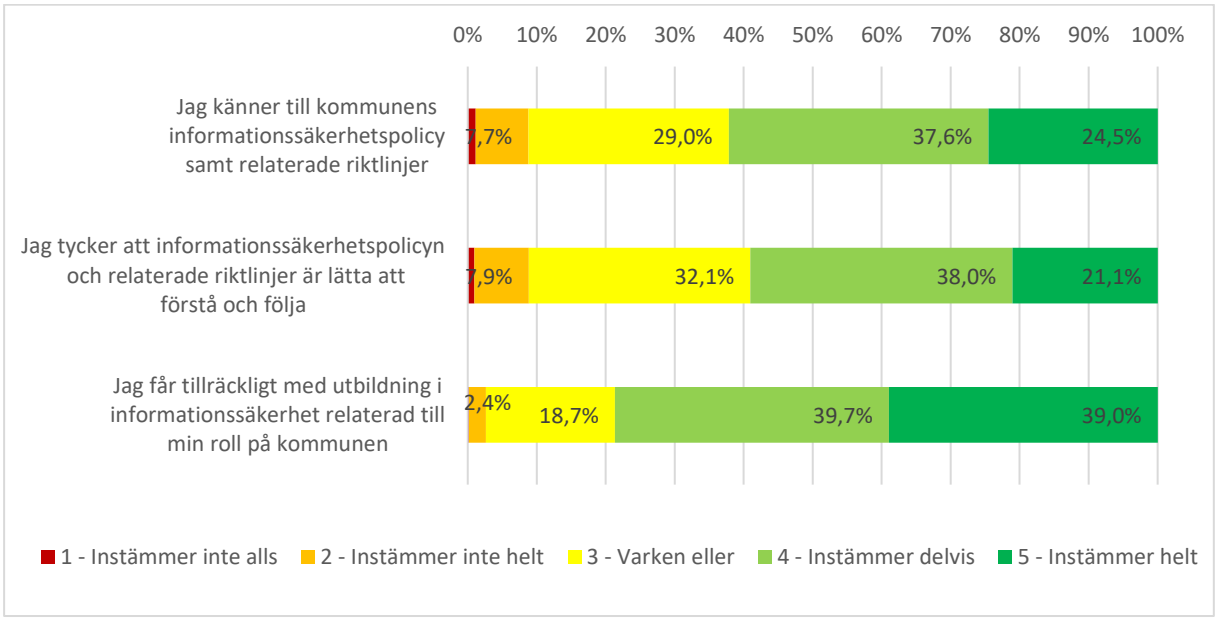
- Jag förstår vikten av att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
- Jag uppmuntras att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
- Jag är medveten om hur och till vem jag ska rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
- Jag känner att jag har gjort något fel när jag rapporterar säkerhetsincidenter orsakade av mig

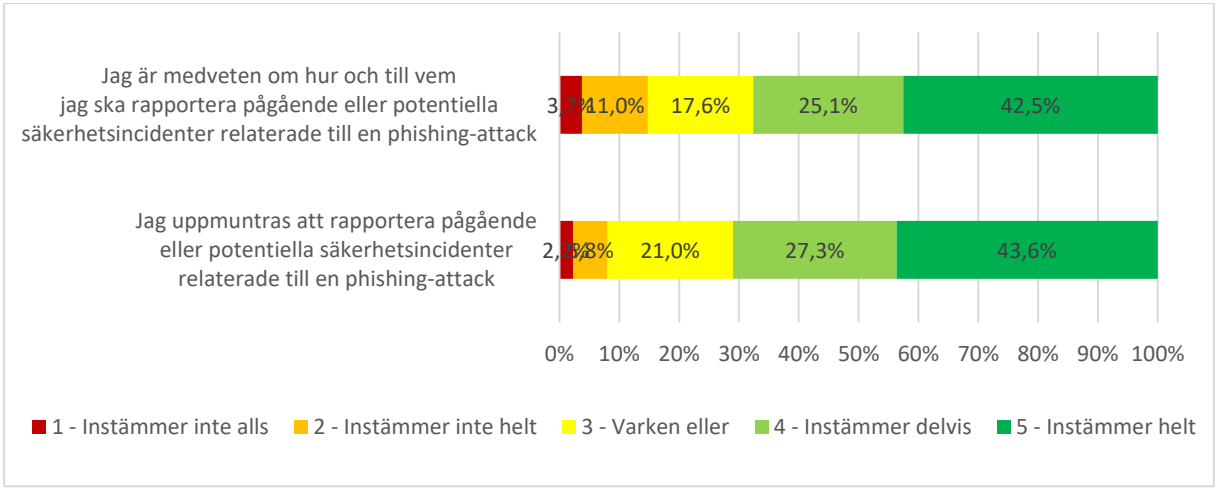
Bilaga 5: Enkätresultat






Rapporterade du e-postmeddelandet?
0%
5%
10%
15%
20%
25%
30%
35%
40%
Ja, jag rapporterade till IT-enheten
18,9%
Ja, jag rapporterade till min chef
2,8%
Nej, men jag kontaktade avsändaren av e-...
0,7%
Nej, jag vet inte hur man rapporterar sådana händelser
5,2%
Nej, jag visste inte att jag skulle rapportera sådana...
12,2%
Nej, då jag insåg att det var en övning såg jag inget...
33,9%
Annat
26,2%


0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Jag känner till kommunens informationssäkerhetspolicy samt relaterade riktlinjer
7,7%
29,0%
37,6%
24,5%
Jag tycker att informationssäkerhetspolicyn och relaterade riktlinjer är lätta att förstå och följa
7,9%
32,1%
38,0%
21,1%
Jag får tillräckligt med utbildning i informationssäkerhet relaterad till min roll på kommunen
2,4%
18,7%
39,7%
39,0%
1 - Instämmer inte alls
2 - Instämmer inte helt
3 - Varken eller
4 - Instämmer delvis
5 - Instämmer helt


Jag är medveten om hur och till vem jag ska rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
11,0%
17,6%
25,1%
42,5%
Jag uppmuntras att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack
21,0%
27,3%
43,6%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
1 - Instämmer inte alls
2 - Instämmer inte helt
3 - Varken eller
4 - Instämmer delvis
5 - Instämmer helt

Bilaga 6: Definitioner

Acceptansnivåer: Acceptansnivåer är ett sätt att översätta generella och övergripande risknivåer till aktuella mätetal som går att följa upp och agera på. Acceptansnivåer bör utgå från organisationens eller företagets kontext, dvs. risknivåer och riskaptit.

Cyberattack: En cyberattack är ett samlingsnamn för olika typer av brott som utförs på IT-system. Attackerna kan utföras för att få tillgång till hemlig information, begränsa tillgången till IT-systemen, samt förstöra data eller IT-system.

Domän: Domän, även kallat domännamn, är en beskrivning av ett namn eller en adress på internet. Vanliga exempel på domännamn är det man skriver in i en webbläsare för att komma till en internetsida eller det som kommer efter "@" i en mailadress, exempelvis "google.com" eller "svt.se".

Falsk avsändare: En falsk avsändare är en avsändare som utger sig för att vara någon den inte är, exempelvis genom att imitera kända e-postadresser eller andra avsändare.

Inbäddad länk: En inbäddad länk är en länk man exempelvis bäddar in i en text eller i en bild, vilket innebär att man kan minska transparensen i att en länk existerar eller vart den leder. Processen är vanlig i phishing-attacker då det ökar mottagarnas benägenhet att trycka på länken.

Intranät: Till skillnad från internet som är tillgängligt för alla är ett intranät ofta privat och bara tillgängligt för den organisation eller företag som äger det. Ett intranät är vanligtvis skyddad från omvärlden av en brandvägg och kan bestå av många sammankopplade lokala nätverk.

IT-infrastruktur: IT-infrastruktur är de komponenter inom en organisation som tillsammans används för att producera, hantera, beräkna, hämta och lagra data. Exempel på detta kan vara en databas eller olika servrar.

Landningssida: En landningssida är en internetsida dit en användare hänvisas efter att exempelvis ha tryckt på en länk eller någon annan form av uppmaning.

Phishing: Phishing, på svenska kallat nätfiske, är en metod för cyberkriminella att attackera privatpersoner, företag och organisationer. Metoden går att utforma på olika sätt men går generellt sätt ut på att lura en mottagare att ladda ner en fil, öppna ett dokument eller trycka på en länk via ett sms eller ett e-postmeddelande. Syftet av phishing-attacker är att utvinna konfidentiell information eller att implementera skadlig kod.

Rate limiting: Rate limiting är en engelsk term som beskriver en inbyggd kontroll som existerar i olika e-postklienter, exempelvis Outlook. Kontrollen begränsar antalet e-postmeddelanden som kan tas emot samtidigt för att förhindra en eventuell överbelastning.

Spamfilter: Spamfilter, även kallat skräppostfilter, är en inbyggd kontroll som existerar i olika e-postklienter, exempelvis Outlook. Kontrollen sorterar alla e-postmeddelanden som en mottagare tar emot och filtrerar ut de e-postmeddelanden som troligtvis är skräppost.

Vitlistning: Vitlistning är en metod företag och organisationer använder för att kontrollera e-posttrafiken. Detta genom att på förhand definiera vilka e-postadresser som är godkända (vitlistade) och på så sätt tillåta kommunikationen.