Examensarbete

IT-forensik och informationssäkerhet

180hp

Quishing i Sikte:

Försvarsstrategier och Verktyg

-En Studie om medarbetares Medvetenhet om QR-kod Phishing och En Undersökning av Anti-Phishing-Verktyg

Halmstad 2024-05-26
Anton Ivarsson & Adrian Stefanescu

HÖGSKOLAN
I HALMSTAD

Quishing i Sikte: Försvarsstrategier och Verktyg

-En Studie om medarbetares Medvetenhet om QR-kod Phishing och En Undersökning av Anti-Phishing-Verktyg

---

Anton Ivarsson & Adrian Stefanescu

Kandidatuppsats
Maj 2024

Akademin för informationsteknologi

Högskolan i Halmstad

Handledare:
Urban Bilstrup

Examinator:
Eric Järpe

Förord

Vi vill uttrycka vår tacksamhet för våra opponenter Emilia och Sanna på Halmstad Högskola för deras värdefulla insatser och bidrag.

Sammanfattning

Denna studie undersöker det växande fenomenet quishing (QR-kod phishing) i ljuset av den ökande användningen av QR-koder under COVID-19-pandemin. QR-koder, som är en lösning för beröringsfri interaktion, har blivit allt vanligare och utnyttjas alltmer frekvent i skadliga phishing-attacker mot företag och deras anställda. Under 2023 observerades en dramatisk ökning på över 2 400 procent i en omfattande quishing-kampanj.

Undersökningen granskar tidigare studier och forskning om quishing och framhäver behovet av att öka medvetenheten bland anställda och hur man kan implementera effektiva skyddsåtgärder. En central del av studien inkluderar en enkätundersökning och en Attack Simulation Training (AST) som genomförs i samarbete med en Managed Security Service Provider (MSSP). Målet med undersökningen är att belysa anställdas medvetenhet om quishing, deras reaktioner och vad som ligger till grund för de anställdas agerande. Vidare inkluderar studien ett experiment rörande hur effektivt MDO (Microsoft Defender for Office) och andra säkerhetslösningar upptäcker inbäddade QR-koder i olika bildformat och rörliga animationer i epost.

Resultaten från enkätundersökningen och ASTn ger insikter som stärker förståelsen för företagens och de anställdas handlande i förhållande till en av många varianter av phishing. Utifrån detta kan rekommendationer för förbättringar, verktyg och policys för att motverka hotet utvecklas och anpassas till hur det verkliga förhållandet är i dagsläget. Studien strävar efter att bidra till en mer omfattande förståelse av quishing och främja framtidens säkerhetskultur inom företagsmiljöer.

Nyckelord: Quishing, QR-koder, Enkätundersökning, Säkerhetsträning, Experiment, MDO (Microsoft Defender for Office 365), Informationssäkerhet, Least privilege, Zero trust.

Innehållsförteckning

Ordlista

Phishing: En typ av cyberattacker där angriparen försöker lura användare att avslöja personlig eller känslig information, vanligtvis genom att utge sig för att vara en betrodd enhet eller person.

QR-kod: En tvådimensionell streckkod som kan skannas med en smartphone eller annan enhet för att få tillgång till information, webbsidor eller andra resurser.

Quishing: En form av phishing där QR-koder används för att lura användare att avslöja känslig information eller interagera med skadlig programvara.

Smishing: En form av phishing där bedragaren använder SMS eller andra meddelandetjänster för att komma över personlig information.

Anti-phishing-verktyg: Program eller system som är utformade för att upptäcka och förhindra phishing-attacker.

Microsoft Defender for Office (MDO): En integrerad säkerhetslösning som syftar till att skydda e-post och samarbetsverktyg, såsom Microsoft Teams, från digitala hot och attacker.

MSSP: En Managed Security Service Provider är en extern leverantör som erbjuder tjänster för företag att outsourca sina säkerhetsbehov. De ansvarar för att övervaka, skydda nätverk och system från cyberhot genom tjänster som inkluderar 24/7 övervakning, intrångsdetektering och sårbarhetsskanning.

Incidentresponsplan: En strukturerad metod för att hantera och svara på en säkerhetsincident, inklusive förebyggande åtgärder och snabb reaktion vid inträffade incidenter.

Säkerhetskultur: En organisations klimat och attityder gentemot säkerhet, inklusive medarbetares engagemang och deltagande i att skydda mot cyberhot.

AI: Konstgjord intelligens, vilket är förmågan hos en maskin eller datorprogram att utföra uppgifter som vanligtvis kräver mänsklig intelligens.

Red teaming: En metod där ett oberoende team simulerar attacker mot en organisations system för att identifiera sårbarheter och utvärdera säkerheten.

AST: En funktion som tillhandahålls av Microsoft Defender for Office 365 Plan 2 för att köra realistiska attackscenarier inom en organisation för att öka medvetenheten och identifiera sårbarheter innan verkliga attacker inträffar.

Kompromitterad: En enhet eller ett system som blivit utsatt för ett säkerhetsintrång och som lett till att obehöriga kan få åtkomst.

CISSP: Certifierad informationssäkerhetsspecialist.

Least privilege: Genom att konsekvent tillämpa principen om minsta privilegium på applikationsnivå kan organisationer skapa en säkrare IT-miljö och isolera kritiska system

1. Inledning

I takt med den digitala utvecklingen har även de metoder genom vilka cyberattacker utförs förändrats och blivit alltmer sofistikerade. En sådan metod är quishing, en form av phishing där QR-koder används som verktyg för att utföra attacker. Användningen av QR-koder har ökat exponentiellt under de senaste åren, särskilt i ljuset av COVID-19-pandemin, vilket har skapat nya utmaningar inom cybersäkerhet. Denna studie syftar till att utforska anställdas medvetenhet om dessa risker samt effektiviteten hos befintliga anti-phishing-verktyg, med ett specifikt fokus på Microsoft Defender for Office. Syftet med denna uppsats är att bidra till en djupare förståelse av hur quishing-attacker uppfattas och hanteras inom organisationer, samt att utvärdera hur väl dagens tekniska lösningar skyddar mot sådana hot. Genom att kombinera en kvantitativ enkätundersökning med en kvalitativ analys av anti-phishing-verktygs effektivitet, avser studien att identifiera eventuella brister i nuvarande försvarsmekanismer och föreslå riktade förbättringar. Denna uppsats är strukturerad enligt följande: Efter inledningen presenteras en teoretisk bakgrund som omfattar tidigare forskning om phishing, med särskilt fokus på quishing. Därefter beskrivs den metod som använts för att samla in och analysera data. I resultat delen redogörs de huvudsakliga fynden från studien, vilket följs av en diskussion där resultaten sätts i relation till tidigare forskning och studiens teoretiska ramverk. Avslutningsvis presenteras slutsatser samt förslag på framtida forskningsområden.

1.1 Bakgrund

Användningen av QR-koder för skadliga ändamål har ökat under COVID-19-pandemin. Utöver hälsoeffekterna påverkade pandemin människors livsvillkor med krav på andningsskydd, distansarbete och kontaktlösa affärer. För att förhindra en snabb spridning av viruset krävdes alternativa metoder för vardagliga interaktioner, vilket bland annat resulterade i användningen av QR som en beröringsfri lösning för att läsa menyer på restauranger eller för att komma in på platser. Trots att QR ursprungligen utvecklades för en snabb metod att förmedla information, var de långt ifrån vardagsbruk innan behovet av beröringsfria interaktioner uppstod. Den snabba förändringen illustrerar hur pandemin accelererat acceptansen och integreringen av QR-teknologin [1], [2].

HRNews (Society for Human Resource Management) rapporterar att det under året 2023 förekom en omfattande phishing-kampanj som involverade quishing [3]. Målen för attackerna var företag och deras anställda, där angriparna simulerade säkerhetsvarningar från Microsoft och uppmanade de anställda att uppdatera sina säkerhetsinställningar. QR-koderna dirigerade användarna till en falsk webbplats, avsedd för att stjäla autentiseringsuppgifter för deras Microsoft-konton. Kampanjen, identifierad av Cofense, noterade en ökning på över 2 400 procent under en fyra månaders period och riktades mot olika branscher inom tillverkning, försäkring, finans, inklusive ett stort amerikanskt energiföretag [4].

Cyberattacker och phishing-försök har eskalerat i frekvens och komplexitet, vilket driver behovet av robustare försvarssystem inom IT-säkerhet. Som en direkt respons på dessa utmaningar har begreppet Zero Trust-arkitektur fått ökad uppmärksamhet som ett viktigt verktyg i kampen mot cyberhot [4]. Enligt en artikel i ProQuest har phishing-attackerna ökat

med nästan 50% från 2021 till 2022, vilket understryker behovet av förändrade säkerhetsstrategier [5].

I boken "CISSP Official (ISC)² Study Guide" av Chapple et al. beskrivs Zero Trust-modellen som baserar sig på strikt verifiering av alla användare och enheter som försöker nå nätverksresurser, oavsett om de befinner sig inom eller utanför nätverkets fysiska gränser. Denna modell inkluderar kontroller och balanser som definieras av en "trusted computing base" (TCB), vilket är en kombination av hårdvara, mjukvara och kontroller som samverkar för att upprätthålla säkerhetspolicyn [6].

Principen om minsta privilegium, Chapple et al. innebär att individer och processer endast ges de behörigheter som är absolut nödvändiga för att utföra sina specificerade uppgifter. Detta begränsar åtkomstnivåerna och minimerar risken för att rättigheter missbrukas eller att skadlig programvara sprids inom systemet. Principen syftar till att förhindra att användare och program får mer omfattande behörigheter än vad som krävs och hjälper till att säkra kritiska system och data från oavsiktlig eller avsiktlig felaktig användning. Genom att strikt tillämpa denna princip kan organisationer effektivt minimera sin attackyta och skydda sig mot interna och externa hot [6].

I en studie om företagsanpassning av webbläsare framgår det att säkerhetskonfigurationer ofta är för generösa, vilket utsätter företagsnätverk för onödiga risker. Forskarna beskriver hur företag kan implementera en strategi där två olika webbläsare används inom samma organisation för att skapa en säkrare miljö: en webbläsare för att ansluta till betrodda interna webbplatser och en annan, med striktare säkerhetskonfigurationer, för att surfa på internet, en så kallad ”least privilege”. Denna åtgärd syftar till att säkerställa att åtkomst till potentiellt skadliga eller opålitliga webbplatser strikt kontrolleras och begränsas. Genom att konsekvent tillämpa principen om minsta privilegium på applikationsnivå kan organisationer skapa en säkrare IT-miljö när användare klickat på skadliga länkar [7].

1.2 Frågeställningar och syfte

Syftet med studiens frågeställningar är att undersöka och belysa den snabba tillväxten av fenomenet quishing, där det efterfrågas mer forskning om hur denna typ av hot kan motverkas. Detta är inte ett nytt hot men har under 2023 blivit mycket relevant och ökat markant, denna uppsats vill skapa och undersöka medvetenhet om quishing samt undersöka kapaciteten av olika anti-quishing verktyg.

1. Vilka strategier och metoder är mest effektiva för att höja medarbetares medvetenhet och engagemang i att förebygga quishing och andra relaterade cyberhot?

2. Hur effektivt är befintliga säkerhetsverktyg, såsom Microsoft Defender for Office, vid upptäckt och blockering av skadliga QR-koder i olika format?

3. Hur kan en organisations säkerhetsåtgärder utformas för att effektivt hantera det växande hotet av quishing med hänsyn till potentiella konsekvenser för företagssäkerhet?

1.2.1 Avgränsningar

Denna studie kommer inte att gå in på hur upprättandet av en phishingsida går till eller tilldelalandet av en unik URL för alla användare utan är mer ett proof of concept gällande animationer.

1.3 Problematisering av frågeställningar

Studiens frågeställningar har flera utmaningar. För den första frågeställningen kan anställdas självrapporterade medvetenhet om quishing vara missvisande, då respondenter ofta ger svar som de tror är socialt önskvärda snarare än korrekta. Detta kan leda till en överskattning av medvetenheten om säkerhetshot.

Att mäta effektiviteten av Microsoft Defender for Office (MDO) verktygets prestation kan skilja sig från verkliga situationer som inte kan replikeras i en kontrollerad testmiljö. Nya och sofistikerade angrepp kan utmana verktygets effektivitet på sätt som inte fullt ut kan förutses.

Slutligen kan företagens förmåga att anpassa säkerhetsåtgärder variera kraftigt beroende på resurser och organisatorisk kultur. Det kan vara svårt att generalisera resultat och rekommendationer utan att ta hänsyn till dessa varierande förutsättningar.

Dessa problematiseringar är viktiga att beakta för att förstå de potentiella begränsningarna i studiens slutsatser och rekommendationer.

1.4 Tidigare forskning om quishing

Utvecklingen inom cyberattacker, särskilt den markanta ökningen av angrepp baserade på QR-kods-phishing (quishing), är oroande. Stu Sjouwerman, VD för KnowBe4 och leverantör av säkerhetsmedvetenhetsträning, understryker att ökningen av denna typ av social manipulation inte borde vara en trend. Emellertid bevisar den ökade användningen av sådana attacker att hotaktörer faktiskt lyckas, annars skulle cyberkriminella inte välja denna metod. QR-koder erbjuder fördelen för angriparen att undgå säkerhetsverktyg, eftersom dessa verktyg inte kan skanna bilden på samma sätt som de kan granska misstänkta URL:er. Dessutom överförs attackvektorn från en säker enhet till en betydligt mindre skyddad enhet, vilket ökar svårigheten att upptäcka intrånget, samtidigt som attackerna utan större besvär kan automatiseras och levereras till en långt större målgrupp [3], [8].

Check Point's Harmony Email team, rapporterade en 587 procents ökning av quishing mellan augusti och september 2023, attackerna anpassar sig dessutom efter användarens operativsystem och skärmupplösning så själva omdirigeringarna till de osäkra URL:erna märks ofta inte av beroende på plattformen som används [9]. Flera företag, inklusive Perception Point och AT&T har sett en markant ökning men tyvärr finns det ett stort mörkertal då inte alla verktyg kan upptäcka den här typen av attacker, särskilt när attacken formar sig efter offrets miljö. Användarutbildning behövs för att öka medvetenheten om quishing, samtidigt som tekniska verktyg, såsom konfigurering av skanningssystem och vitlistning/svartlistning av e-postdomäner, bör implementeras. Simulerade attacker, inklusive QR-koder, rekommenderas som en del av red teaming för att utvärdera försvar och reaktioner. Användning av AI, särskilt bildigenkänningsteknik, behöver utvecklas för att upptäcka dessa attacker [9], [10].

Den signifikanta tillväxten motiverar en närmare granskning och utveckling av strategier för att öka medvetenheten bland anställda och företag om riskerna med quishing. Det är särskilt viktigt att notera att denna form av attacker har intensifierats sedan början av covid-19-pandemin, vilket gör det ännu viktigare att utveckla och implementera effektiva skyddsåtgärder [1].

F. Sharevski et al. genomförde en studie där de använde en falsk QR-kod i en COVID-19-passregistrering och fann att 67 procent av deltagarna var benägna att dela sina Google- eller Facebook-uppgifter av bekvämlighet. En Quishing Awareness Scale (QAS) konstruerades för att mäta medvetenheten om quishing, och resultaten användes för att föreslå träningsriktlinjer och testa säkerhetsindikatorer för att varna användare om QR-kod phishing. De underströk vikten av att höja medvetenheten genom att föreslå säkerhetsriktlinjer för att motverka quishing [1].

Att hantera den mänskliga faktorn och medarbetares kunskaper utgör en betydande utmaning inom säkerhetsarbetet för varje organisation. I de rapporter som skickas till MSB framhålls nätfiske och svaga lösenord regelbundet som de främsta orsakerna till hur en angripare får den inledande åtkomsten till en organisations informationssystem [11].

Likaså måste även olika datormodeller utvecklas för att detektera användare som skannar en QR-kod. I en studie med två olika experiment, kom man fram till att i det första experimentet hade 75% av mottagarna skannade QR-koden av ren nyfikenhet och ytterligare 85% besökte en phishing sida i det andra experimentet [12]. H. Wahsheh och M. Al-Zahrani genomförde en studie för att detektera skadliga webblänkar i QR-koder genom att använda två datormodeller, fuzzy logic och multilayer perceptron artificial neural network (MLP-ANN). Efter att ha jämfört resultaten valdes MLP-ANN som den bästa modellen för att upptäcka skadliga URL:er i QR-koder. De utvecklade en prototyp av en realtids scanner för att skanna skadliga QR-koder, kallad BarCI. Scannern baserades på MLP-ANN och visade sig ha en 82,9% effektivitet vid detektering av skadliga URL:er [13].

I studien ” QsecR: Secure QR code Scanner According to a Novel Malicious URL Detection Framework” föreslås det att man kan stärka företagens långsiktiga ekonomi och säkerhet genom forskning som främjar användningen av uppdaterad mjukvara samt extern mjukvara för att upptäcka hot som kringgår traditionella säkerhetslösningar. Studien exemplifierar den särskilda betydelsen av avancerade QR-kodsskannrar, som QsecR, vilka använder en kombination av maskininlärning och svartlistningsmetoder för att identifiera skadliga URL:er. Dessa tekniker är speciellt effektiva mot hot som ofta missas av konventionella system [14].

1.5 Tidigare forskning om phishing och metoder

I studien ”Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation” genomförde forskare en uppföljning av anställda i ett företag som nyligen hade genomgått en phishingsimulering. Forskarna bad de anställda att delta i en enkät som inkluderade uppgifter för att upptäcka olika slags phishing. De anställdas beteende klassificerades under simulationen, om de rapporterade

det misstänkta e-postmeddelandet eller om de varken rapporterade eller klicka på länken i mailet alternativt om de interagerade med länken [15].

I en experimentell studie [16] analyserades effektiviteten av anti-smishing-tekniker (Anti SMS-Phishing-tekniker) från bulkmeddelandeservrar, mobiloperatörer och anti-smishing-applikationer som skulle filtrera bort kända smishing-meddelanden. Resultaten forskarna kom fram till indikerade på områden där förbättringar krävdes för att bekämpa smishing-attacker. Studien gav perspektiv på teknologiska svagheter och identifierade förbättringsområden inom bekämpningen av olika typer av mobila bedrägerier och belyser några gemensamma säkerhetsutmaningar jämfört med quishing. Därmed kan utvecklingen av säkerhetsskydd mot olika typer av bedrägerier inom mobila kommunikationstjänster främjas. Båda bedrägerierna förlitar sig på människors sårbarhet där mänsklig psykologi och social manipulation utnyttjas för att lura användare att interagera med bedrägliga meddelanden eller QR-koder. Båda typerna av bedrägerier kräver att användare är medvetna om riskerna och tar förebyggande åtgärder. Utbildningsinitiativ för att öka medvetenheten om säker mobilanvändning kan vara en gemensam strategi.

Studien "Spears Against Shields: Are Defenders Winning the Phishing War?" [17] är en djupgående analys av phishing och försvarsverktyg där man undersökte effektiviteten av populära anti-phishing verktyg. Studien genomfördes genom att generera 1,000 phishing-e-postmeddelanden med hjälp av natural language generation (NLG) där forskarna kunde undersöka detektionen av dessa hot jämfört med fem välkända antivirusprogram med anti-phishing funktioner. Resultaten visade att antalet oupptäckta phishing meddelanden i form av epost varierade kraftigt mellan de olika verktygen, en kraftig spridning med detektionsgrader från 6% oupptäckt phishing till så mycket som 93% ej upptäckta hot i epost. Man utforskade även effektiviteten av olika träningstekniker mot phishing genom att analysera hur väl dessa verktyg lyckades öka medvetenheten och förmågan att identifiera phishing bland anställda. Man kom fram till att trots tillgång till sofistikerade verktyg och träning, fortsatte phishing-attackerna att vara framgångsrika, vilket understryker behovet av ytterligare förbättringar inom både tekniska lösningar och utbildningsmetoder. Detta framhäver en viktig aspekt av cybersäkerhet som är direkt relevant för organisationer som måste skydda sig mot cyberattacker.

1.6 Studiens unika bidrag

Studiens frågeställningar skiljer sig från tidigare forskning genom att kombinera två viktiga aspekter inom cyberhot: anställdas medvetenhet om QR-kod phishing (quishing) och effektiviteten av specifika anti-phishing-verktyg. Tidigare studier har främst fokuserat på enskilda aspekter som medvetenhetsträning eller teknologiska lösningar för att bekämpa phishing.

Genom att undersöka både medvetenheten och verktygets effektivitet inom samma företagsmiljö, strävar studien efter att ge en mer omfattande förståelse för hur företag kan skydda sig mot quishing-attacker. Studien undersöker Microsoft Defender for Office 365 som är ett väl etablerat skyddsverktyg. Effektiviteten utvärderas med hjälp av en kvantitativ

enkätstudie och dess effektivitet i verkliga scenarier i jämförelse med andra befintliga verktyg med hjälp av ett experiment.

Det unika med studiens frågeställningar ligger i att vi inte bara analyserar verktygens tekniska effektivitet utan också hur medvetenheten hos anställda påverkar den övergripande säkerheten. Denna holistiska metod erbjuder nya insikter och rekommendationer för att utveckla mer effektiva strategier för att bekämpa quishing-attacker.

1.7 MDO

Microsoft Defender for Office 365 är ett integrerat skydd som prioriterar e-post och samarbetsverktyg, såsom Microsoft Teams. Med över 65 biljoner dagliga analyser av säkerhetssignaler och blockering av över 70 miljarder e-post- och identitetsattacker under 2023 erbjuder MDO ett omfattande skydd för företag mot digitala hot. Risken för e-postintrång minskade med 29%, genomsnittlig undersökningstid minskade från 12 timmar till 1 timme och tiden för att blockera skadliga länkar minskade med 95% [18].

1.8 AST

Attack Simulation Training (AST) är en funktion tillgänglig för organisationer med Microsoft Defender for Office 365 Plan 2. Syftet är att köra realistiska attackscenarier inom organisationen för att identifiera och hitta sårbara användare innan verkliga attacker inträffar.

För att använda AST krävs en licens för antingen Microsoft 365 E5 eller Microsoft Defender for Office 365 Plan 2. Åtkomst till AST ges genom Microsoft Defender-portalen, där det specifika läget för AST finns under "Email and collaboration > Attack simulation training" eller direkt via länken https://security.microsoft.com/attacksimulator.

För att utföra AST-procedurer krävs specifika roller som Global Administrator, Security Administrator, Attack Simulation Administrators, och Attack Payload Author. Microsoft Entra-behörighet krävs också.

Det finns ingen motsvarande PowerShell-cmdlet för AST. Data från AST lagras tillsammans med annan kunddata för Microsoft 365-tjänster och är tillgänglig i regioner som APC, EUR och NAM.

AST inkluderar olika simuleringar för social engineering-tekniker såsom Credential Harvest, Malware Attachment, Link in Attachment, Link to Malware, Drive-by-url och OAuth Consent Grant [19] samt två stycken lärande moduler för hur en kan detektera och undvika skadliga QR-koder[20].

Simuleringarna inom AST syftar till att träna organisationens användare mot olika former av phishing och andra hot. AST är tillgänglig i olika Microsoft 365-prenumerationer, och tillgängligheten i specifika miljöer och regioner varierar.

Sammanfattningsvis är AST en omfattande funktion som tillhandahålls av Microsoft Defender for Office 365 Plan 2 för att simulera olika attackscenarier, särskilt inom området phishing, för att öka medvetenheten om säkerhet och identifiera potentiella sårbarheter. Användare med rätt behörigheter kan få tillgång till och hantera AST via Microsoft Defender-portalen [19].

2. Metod

En enkätstudie, ett experiment och en attack-simulation låg till grund för de vetenskapliga metoderna som gjorde det möjligt att få svar på studiens frågeställningar genom en kombinerad metodik och som beskrivs här. För att adressera de identifierade problemen skapades en metodologi där en extern aktör specialiserad inom hantering av säkerhetstjänster, en Managed Security Service Provider (MSSP), ansvarade för att utföra en Attack Simulation Training (AST) mot ett företag inom fordonsindustrin. En del utav deltagarna i ASTn länkades till vårt formulär för att besvara studiens enkätfrågor. Det skapades en experimentell design med testfall av kända URL:er och quishing-URL:er som utvärderade MDO:s och andra verktygs prestanda för att besvara frågeställningen om MDO:s effektivitet mot inbäddade QR-koder.

2.1 Enkätundersökning

Det genomfördes tre AST för att utvärdera effekt av den första simuleringen i frågan om den anställde klickat respektive rapporterat mejlet, likt Beu et al. beskriver, och i samarbete med det berörda företaget inom fordonsindustrin inkluderades en heltäckande enkätundersökning [15]. Undersökningen länkades från den aktuella AST:n genom att utvalda användare fyllde i ett Microsoft forms formulär som en del av studiens surveydesign.

Det skapades tydliga instruktioner för att underlätta för respondenten att förstå frågorna då hen läser frågorna själv eftersom vårt forskningsinstrument saknade en aktiv intervjuare. Därigenom minskade risken för skevheter för socialt önskvärda svar. Dessutom lämpar sig studiens metodval bättre vid undersökningar där det kommer att ställas känsligare frågor, vilket också betonas i litteraturen. Frågornas antal hölls nere för att undvika trötthet och ett för högt bortfall. Enkäten skapades med relevanta och i huvudsak slutna frågor men inkluderade också likertskalor, bilder och animationer [21]. Det gjordes detaljerade mätningar av hur användaren betygsätter sin medvetenhet, kännedom, lojalitet mot företaget och antalet år den anställde arbetat på sitt företag. En positiv inställning gentemot företaget kan skapa incitament och har en betydande påverkan för sannolikheten att upptäcka äkta phishing samt avstå från att klicka på länkar och av lika stor vikt att anmäla det maliciösa meddelandet [15].

Det gjordes analyser om underliggande faktorer som påverkar de anställdas beslut samt det som motiverat deras agerande. Medvetenheten av fenomenet quishing, undersöktes samt förekomsten av incidenter och hur allvarligt det uppfattades av de anställda.

Genom att det utfördes en enkätundersökning i kombination med en attacksimulation kunde det bidra till att få en mer omfattande bild av deltagarnas reaktioner och attityder gentemot phishing-attacker och därigenom gjorde det studiens forskningsresultat mer robusta och informativa. Det inkluderades flera frågor som syftar till att fånga olika aspekter av deltagarnas upplevelse och uppfattningar kring phishing-attacker och företagets säkerhetskultur. Varje fråga konstruerades med noggrannhet för att säkerställa relevans och användbarhet för att uppfylla forskningsmålen.

Medvetenhet och Erfarenhet av Phishing: För att förstå den generella medvetenheten och eventuella tidigare erfarenheter av phishing-attacker inom organisationen, inkluderades en

fråga som direkt frågar deltagarna om de någonsin varit medvetna om eller upplevt phishing-attacker under sin tid på företaget.

Typ av Phishing-attacker: För att identifiera vanliga angreppsmetoder inkluderades en fråga som uppmanar deltagarna att specificera vilken typ av phishing-attacker de har stött på. Detta ger insikt i vilka angreppsvägar som är vanligast och därmed vilka områden som kan kräva ytterligare uppmärksamhet och utbildning.

Påverkan av Utbildningsbakgrund: För att undersöka om utbildningsbakgrund kan påverka förmågan att känna igen och undvika phishing-attacker inkluderades en fråga som ber deltagarna reflektera över hur deras utbildningsbakgrund kan ha påverkat deras förmåga att hantera sådana hot.

Utvärdering av Företagets Träningsprogram: För att bedöma effektiviteten av företagets tränings- och resursprogram för att förebygga och hantera phishing-incidenter inkluderades en fråga som direkt frågar deltagarna om de anser att företaget tillhandahåller tillräcklig träning och resurser i detta avseende.

Självförtroende i att Identifiera Phishing-attacker: För att bedöma deltagarnas självförtroende i sin förmåga att identifiera och undvika phishing-attacker inkluderades en fråga som direkt ber deltagarna att utvärdera sitt eget kunskaps- och självförtroendeläge.

Vikt av Säkerhetsmedvetenhet: För att undersöka deltagarnas syn på vikten av att vara försiktig och vaksam mot phishing-attacker inkluderades en fråga som uppmanar deltagarna att uttrycka sin uppfattning om ämnet och därmed belysa hur medvetenhet om säkerhet värderas inom organisationen.

Rapportering av Phishing-försök: För att bedöma deltagarnas benägenhet att rapportera phishing-försök inkluderades en fråga som direkt frågar om de någonsin har rapporterat ett sådant försök, vilket är avgörande för incidenthantering och stärkande av övergripande cybersäkerhetsåtgärder.

Företagets Säkerhetsåtgärder och Anställdas Lojalitet: För att få insikt i deltagarnas uppfattningar om företagets engagemang för säkerhet och dess inverkan på deras lojalitet och engagemang inkluderades en fråga som ber dem uttrycka sina åsikter i detta avseende.

QR-kod Phishing: För att undersöka förekomsten och uppfattningen om QR-kod phishing inkluderades en fråga som direkt frågar om deltagarna har stött på sådana attacker och deras upplevelse av dem.

Microsoft Defender for Office 365 (MDO) och liknande säkerhetsverktyg: För att bedöma upplevelsen av verktygens effektivitet att upptäcka och hantera potentiella phishing-hot inkluderades en fråga som direkt ber deltagarna att utvärdera den upplevda prestandan baserat på deras eller andra anställdas erfarenhet av verkliga incidenter.

Målet med dessa frågor var att de kommer att ge oss en djupare förståelse för deltagarnas upplevelser och attityder gentemot phishing-attacker och företagets säkerhetskultur, vilket kommer att vara värdefullt för studiens forskning och för att identifiera områden för förbättring i företagets säkerhetspraxis.

Genom samarbetet med MSSP vid utförandet av en AST utfördes en efterföljande enkätstudie, och det skapades en holistisk metodik. Denna tvåstegsansats möjliggjorde en kvantitativ och kvalitativ analys av de anställdas reaktioner på phishing-simuleringar. Resultaten av denna undersökning gav insikter och bidrog till en djupare förståelse för både företagens handlingsmönster och de anställdas medvetenhet och attityd till quishing, vilket i sin tur gav ett underlag för en mer omfattande och nyanserad slutsats som ledde till nya insikter och förslag till policys eller andra förbättringar som kan motverka quishing.

Det planerades att antalet respondenter i enkätundersökningen skulle komma att sträcka sig till flera tusentalet respondenter. Denna omfattande respons hade kunnat styrka validiteten av denna undersökning och ge en bredare förståelse för företagens handlingsmönster och de anställdas medvetenhet om quishing och hur man ytterligare kan öka medvetenheten bland anställda.

Metodologin innefattade en utforskning av befintliga teorier och studier med avsikt att förvärva insikter angående den befintliga kunskapsbasen inom det valda forskningsområdet. Målet var att konkretisera studiens forskningsfrågor för att hitta ett syfte med frågorna och undvika redundans av tidigare genomförd forskning. Detta bidrog till en solid grund för den informationsinhämtning som genomfördes [21], [22].

2.1.1 Enkätfrågor

Enkätfrågorna måste följas av en bra motivering med syftet med undersökningen och varför det är viktigt för respondenten att medverka. Metoderna som valdes syftar till att utforska hur vanligt phishing och quishing är, hur anställda reagerar och agerar i sådana situationer och hur faktorer som lojalitet mot företaget, utbildningsnivå och anställningstidens längd påverkar deras förmåga att identifiera hot samt deras vilja att skydda företaget. En komplett lista över frågorna finns tillgängliga i Appendix A.

2.1.2 Urval

Från den totala gruppen av anställda som deltog i Attack Simulation Training (AST) via MSSP, valdes slumpmässigt 100 stycken deltagare ut för att delta i enkätundersökningen. Urvalet skedde utav MSSP för ett ”Automotive Industry” företag, där respondenternas antal, nationalitet och yrkesroller valdes slumpmässigt och anpassades enligt studiens avgränsningar och inklusionskriterier vid tidpunkten för datainsamling. En av inklusionskriterierna var att deltagarna skulle vara personer som regelbundet hanterar e-post i en företagsmiljö, vilket är kritiskt för att hålla studiens fokus på quishing.

2.2 Experiment

Denna studie utforskade också effektiviteten hos Microsoft Defender for Office (MDO) för att identifiera och neutralisera phishing-angrepp. Det skedde en registrering av ett Microsoft E5-utvecklarkonto för att skapa en kontrollerad utvecklingsmiljö som simulerade ett företagsnätverk i molnet med fiktiva användare. Inom denna miljö genomfördes en serie systematiska tester för att utvärdera MDO:s förmåga att upptäcka och filtrera ut phishing-försök. Tre andra verktyg valdes också ut för att jämföra effektiviteten i realtid mellan säkerhetsföretagens möjlighet och att blockera skadliga QR-koder. Resultaten registrerades och

dokumenterades noggrant, inklusive korrekt identifierade legitima QR-koder, korrekt identifierade bedrägerikoder, falska positiva och falska negativa. Träffsäkerhet, känslighet och specificitet beräknades för att bedöma verktygets förmåga att korrekt identifiera och hantera bedrägliga QR-koder, vilka jämfördes med URL- och filanalysverktyget virustotal.com. De skadliga länkarna hämtades från phishtank.org och kriterierna för att en URL skulle anses som skadlig var att webbplatsen aktivt begärde användarnamn och lösenord från en domän som inte tillhör företaget. URLn fick inte vara äldre än två dagar, från det att den blev inrapporterad på phishtank.org. Länken skulle också få minst fyra träffar på virustotal.com och att webbplatsen fortfarande skulle vara tillgänglig vid tiden för experimentet. För att simulera verkliga scenarion, och mäta effektiviteten implementerades tre huvudsakliga teststrategier:

- Skicka e-post med klartextade phishing-URL:er för att bedöma MDO:s förmåga att detektera direkttextade hot.
- Integrera dolda phishing-URL:er, kodade som QR-koder i statiska bildformatet png, för att utvärdera MDO:s skanningskapacitet av bilagor för att identifiera och avlägsna hot.
- Integrera dolda phishing-URL:er, kodade som QR-koder i animerade bildformatet gif, för att utvärdera MDO:s skanningskapacitet av bilagor för att identifiera och avlägsna hot.

Det valdes ut 16 skadliga länkar som var högst tre timmar gamla. Det valdes också ut 16 harmlösa länkar baserat på deras placering i Fortune Global 500-listan [23]. En genomgång av 2023 års upplaga av listan gjordes och erhölls direkt från Fortune Magazine's officiella webbplats. Vårt urval fokuserade specifikt på företag med en stark global närvaro, vilket motiverades av antagandet att dessa företag skulle ha välutvecklade, giltiga och erkända inloggningsportaler.

Urvalsprocessen inleddes med det högst rankade företaget på listan och fortsatte nedåt tills 16 företag hade identifierats. För varje potentiellt företag utfördes en noggrann kontroll för att verifiera att en direkt tillgänglig inloggningsportal fanns på deras officiella hemsida. Detta steg var avgörande för att säkerställa äktheten och säkerheten hos de valda portalerna, och endast officiella företagswebbplatser undersöktes. Om ett valt företag saknade en direkt tillgänglig inloggningsportal på sin publika webbplats, anpassades metoden genom att gå vidare till det näst högst rankade företaget på listan. Denna flexibla men systematiska ansats säkerställde att vårt slutliga urval enbart bestod av företag med lättillgängliga och säkra inloggningsportaler. Varje steg i urvalsprocessen dokumenterades för att upprätthålla studiens transparens och möjliggöra replikering. Varje testfall fick ett TestID och kategoriserades enligt kriterierna om det var skadlig, blockerat av MDO när det skickades i klartext eller om det genererades en miniatyrbild i meddelandet som skickades eller skrevs. Det noterades också uppgifter för de statiska QR-bilderna och QR-animationerna.

Information om detektering, falsk positiv, falsk negativ och korrekt QR räknades ut. Förutom ett TestID behölls Phishtank.org ID-nummer, Fortune Global 500 placeringen och antalet träffar för respektive länk på VirusTotal.com registrerades. Förutom MDOs statistik antecknades det hur andra verktyg klassificerade QR-koderna i var sitt fält: Eset Premium Edge extension, Trend Micro QR scanner för Android, Kaspersky för Android och om de lyckades att blockera eller varna användaren korrekt.

2.2.1 Experimentuppställning

Testdatorn för att kontrollera phishinglänkarna var en Lenovo B590 med en Intel i5 3230m, 8 GB RAM och operativsystemet CAINE 13.0 som exekverades som en Live USB för att isolera enheten till det yttersta från resten av laptoppens maskinvara. För att undvika att routern blockerade trafiken upprättades en hotspot där en mobiltelefon med en mobil internetanslutning delade sin tunnlade internetanslutning genom VPN-tjänsten Mullvad.

Ett manuell skapande av individuella QR-koder, där en laddningsanimation som sedan skulle sammanfogas med en individuell QR-kod skulle bli en tidskrävande process för att skapa en unik kod för alla användare och följaktligen utföll detta och processen automatiserades.

Jämförelser gjordes av effektiviteten med en metod som förekommer i studien om smishing [16] och som ger en vägledning i testning av kapaciteten av skyddsverktyg mot phishing. Metoderna i studierna som Wahsheh [13] och Rafsanjani [14] använder kommer att vägas in i studiens utvärdering av MDO.

2.2.2 Forskningsdesign

För att skala upp framställningen av meddelanden likt det som gjorts i delar av de tidigare studierna, implementerades automatiseringsprocessen med ett Python script skapat av författarna av studien (Appendix B). Scriptet importerade en addresses.cvs-fil med e-postadresser som skulle inkluderas i den animerade QR-koden. Därigenom skapas en individuell animation för varje användare med användarnamnet som filnamn. Animationen bestod av tolv svarta cirklar som snurrade medurs runt ”Loading” texten och visades de första sex sekunderna för att sedan visa en QR-kod (se fig. 1). För att lättare skicka bulkmeddelanden med hjälp av Microsoft Graph (API) och ökad känsla av realism och äkthet för mottagaren, implementerades funktioner för att underlätta individualisering av meddelanden genom att koda in användarnamnet i själva URL:en för phishing sidan med Base64.

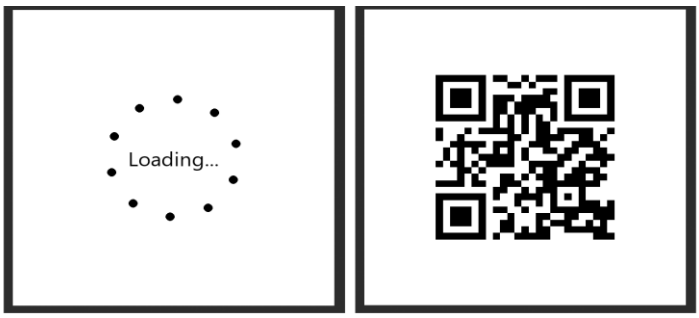

Fig. 1. Färdig animation med sammanfogad animation och QR-kod i en fil, här ses www.example.com.

2.2.3 Beräkning av träffsäkerhet, känslighet och specificitet

För att beräkna dessa värden med 16 skadliga och 16 icke skadliga länkar som kontrollerades tre gånger var, användes följande formler:

Träffsäkerhet: (Antal korrekta identifieringar av skadliga länkar + Antal korrekta identifieringar av icke-skadliga länkar) / Totalt antal tester.

Känslighet: Antal korrekta identifieringar av skadliga länkar / Totalt antal skadliga länkar.

Specificitet: Antal korrekta identifieringar av icke-skadliga länkar / Totalt antal icke-skadliga länkar.

2.2.4 Verktyg och programvara

Under arbetet har en rad olika verktyg och programvaror använts för att samla in data, analysera resultat och hantera referenser:

Microsoft Word: Huvudverktyget som använts för dokumentredigering och sammanställning av denna uppsats.

Zotero: Användes för att organisera och hantera bibliografiska referenser, vilket förenklade citeringsprocessen och säkerställde korrekt referenshantering.

Microsoft Excel: Nyttjades för att samla in och analysera data, vilket möjliggjorde en effektiv bearbetning av statistik och resultat.

Matplotlib: Detta bibliotek för Python användes för att skapa visualiseringar av data, vilket hjälpte oss att tydliggöra trender och mönster i undersökningen.

Microsoft Forms: Verktyget användes för att designa och distribuera enkäter. Detta underlättade insamlingen av data från respondenter på ett strukturerat sätt.

YouTube: Plattformen användes för att publicera en instruktionsvideo kopplad till studiens enkät, vilket bidrog till att öka engagemanget och förståelsen bland deltagarna.

Microsoft PowerPoint: Användes för att skapa och designa presentationer av vårt forskningsarbete för att på ett effektivt sätt kommunicera studiens resultat och analyser till en bredare publik, vid seminarier.

Dessa verktyg har varit centrala för att effektivisera vårt arbete och säkerställa hög kvalitet på den insamlade datan samt slutprodukten av studiens forskning.

2.3 Etiska överväganden

Det sågs till att alla deltagare i enkätundersökningen informerades om syftet med studien och deras deltagande var frivilligt. Deras integritet och anonymitet respekterades genom att inga personligt identifierbara uppgifter samlades in. Datainsamlingen och hanteringen följde gällande lagar och regler för integritetsskydd och etik inom forskning. Det sågs till att resultaten av studien används på ett ansvarsfullt sätt och för att främja förbättringar inom cybersäkerhetsområdet utan att skada individers eller företags integritet.

2.4 Positionering

Denna uppsats positionerar sin forskning som ett bidrag till förståelsen av företags reaktioner på phishing-attacker och effektiviteten hos verktyg som Microsoft Defender for Office 365 (MDO). Genom att kombinera enkätundersökningar med en Attack Simulation Training (AST) eftersträvas det en holistisk bild av företagens säkerhetskultur och de anställdas medvetenhet om phishing-hot. Uppsatsen erkänner utmaningar och begränsningar med dess metod och erbjuder förslag för framtida forskning inom området.

2.5 Problematisering av metod

Mätningsvaliditeten av anti-quishing-verktygets effektivitet och anställdas reaktioner på simuleringen kan skilja sig från verkliga hot. Konsekvenserna för quishing kan bli svåra att tolka och komplext. Metoden som valdes med enkätstudie skulle möjligen kunna ersättas av kvalitativa intervjuer med experter på företagen. Metoden har potential att erbjuda en mer detaljerad förståelse än enkätundersökningar och kan vara praktisk för att identifiera särskilda konsekvenser och förbättringsområden. Samtidigt är det inte säkert att det skulle erhålla ett tillräckligt högt deltagande för att få en pålitlighet och därmed någon validitet [21] i uppsatsens slutsatser vilket motiverar användningen av enkätundersökningar för att säkerställa ett mer omfattande deltagande och datainsamling.

Ett annat tänkvärt fenomen som kan uppstå när en uppsats använder sig av enkätstudie är dessutom att respondenterna kan vara benägna att ge socialt önskvärda svar för att följa policys eller andra normer inom företaget, vilket kan påverka validiteten av resultaten. En utmaning är att attack-simulationen vid tillfället för ASTn inte har en inbyggd modul för quishing-simuleringar. Möjligheten att skapa en fungerande simulering av studiens författare fanns och erbjöds till MSSP men risken för att företagen skulle få eventuella bortfall av mätvärden gjorde detta alternativ osäkert. Experimentet med dolda URL:er begränsades av att denna fråga är en del av ett arbete och gick inte in på djupet med många exempel. Ett mindre antal QR-koder genererades med animationer på grund av nuvarande tidsåtgång för att skapa animationerna med maliciösa adresser. Kärnan i studiens undersökning var att undersöka verktyget som företaget använde som säkerhet undertiden vi samlade in en mer nyanserad kunskap genom studiens enkät. Detta experiment är ett försteg till att motivera framtida forskning när det kommer till området om vad som kan förbättras med maskininlärning för att upptäcka hot som spelar på denna typ av social engineering.

3. Resultat

3.1 Enkätundersökning

Resultaten från enkäten som hade 83 respondenter kommer presenteras fråga för fråga under denna rubrik. Fullständiga frågor samt svarsalternativ finns att läsa i Appendix A.

För att få svara på samtliga frågor mellan fråga 6-21 i undersökningen så var respondenten tvungen till att svara "Yes" på fråga fem då denna tog upp om den svarande hade råkat ut för några phishing-försök under sin tid på företaget. Om respondenten inte hade råkat ut för försök av denna sort eller blivit medveten om phishing så fanns det ingen relevans för personen att besvara fråga 6-21 då dessa direkt berör individens hantering, uppfattningar och tankar kring dessa phishing-försök. Detta gjordes alltså för att förenkla och effektivisera undersökningens syfte i form av att det ökar svarsfrekvensen när respondenten inte behöver svara på frågor som det ändå inte är relevant att de besvarar. Det bidrar även till ett lägre antal bortfall i studiens enkätsvar av just samma anledning.

3.1.1 Svar på enkät-frågorna

Här kommer ni kunna läsa samtliga frågor och dess svar. För att förenkla läsbarheten är de frågor där respondenten skulle svara med fri text, utskrivna i löpande text. De frågor som var av formatet flerval eller där respondenten skulle svara på en skala, är infogade som figurer där både frågorna och svaren kan ses.

Fråga 1. Fråga om hur länge respondenten jobbat på det företag där de har sin nuvarande anställning:

Medelvärde över anställningstiden uppgick till 7.6 år och medianen var 3 år.

Fråga 2. Fråga om vad respondenten har för roll på sitt företag:

Här finns det ett visst bortval av personer som inte gett ett fullständigt eller konkret svar. De svaren som exempelvis "0" kommer därav sorteras bort för att undvika förvirring vid läsande av listan. Det är även för att förbättra flödet i listans uppbyggnad. Komplett lista på dessa svar som även inkluderar svar som anses felaktiga finns att läsa i Appendix B.

1 Ekonomi-assistent
2 Säljare
3 Assistent
4 Soc analytiker
5 VD
6 Chef
7 Tillsvidareanställd
8 HR
9 Ekonomi

10 IT
11 Projektchef
12 Nättekniker
13 CFO
14 Ekonomiassistent
15 Kassaledare
16 Studentmedarbetare
17 Studentmedarbetare
18 Unified Production & Logistics worker
19 Software Developer
20 IT
22 Säkerhetsanalytiker
23 Incidenten och Problemmanager
24 Enhetschef
25 Sekreterare
26 Administratör
28 Snickare
30 Vd
33 Projektledare
34 Läkare
35 Administratör
36 Tekniker
40 Kurator
41 AT-läkare
42 Account manager
43 Mekaniker
44 Redaktör
45 Lagerarbetare
46 Projektledare elkraft
47 Undersköterska
48 Första linjens chef
51 Undersköterska
53 Operatör
54 Consultant
55 Administration och patient behandling.
56 Universitetsadjunkt
57 Undersköterskan
58 Chaufför
59 Marketing
61 Varumottagning
64 Cyber Security Consultant
65 Manufacturing Engineering
66 Specialist
67 Customer Care

68 IT Cybersecurity Expert
69 Business Transformation & Retailer Development
70 R&Dengineering
71 Developer
72 Homologation
73 Union representative
74 Adjunkt lärarutbildningen
75 Data Architect in Digital Core
76 Leading function in Supply Chain
77 HR Manager
78 Design leader
79 Test engineer
80 Senior Site-SPM Engineer
81 Secure Identity Techlead
82 CISO
83 Biomedicinsk analytiker

Fråga 3. Fråga om respondentens åldergrupp. Totalt 83 svar:

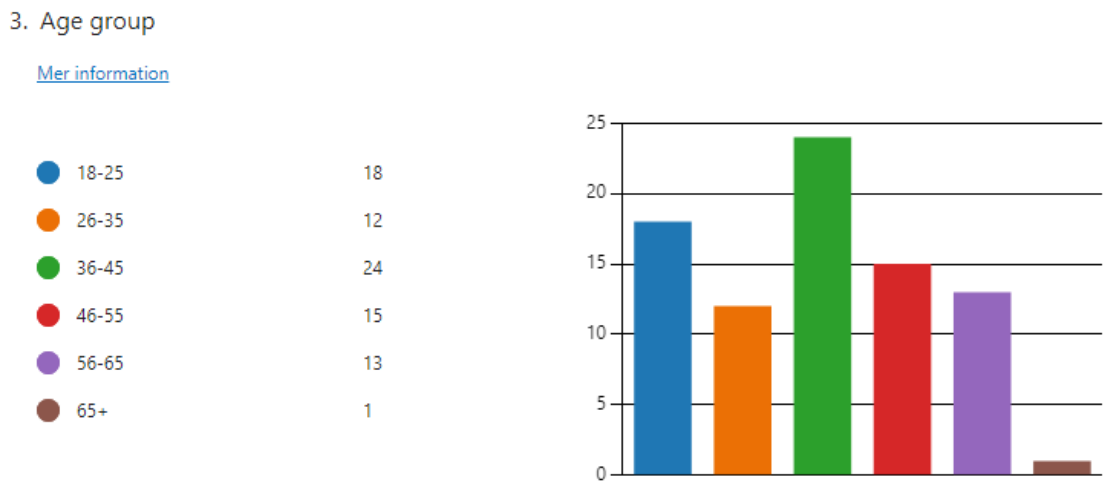

Fig. 2. Resultatdiagram fråga 3 enkät

Fråga 4. Fråga om respondenten har någon form av IT utbildning. Första frågan som inte syns i sin helhet är Intern utbildning inom företaget. Totalt 83 svar:

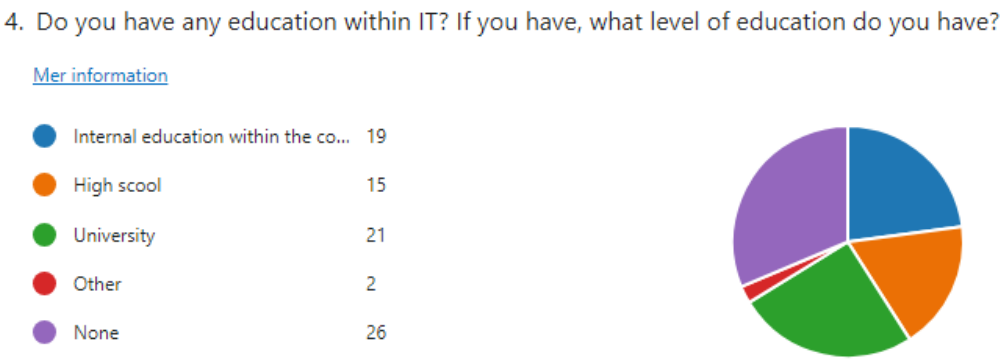

Fig. 3. Resultatdiagram fråga 4 enkät

Fråga 5. Fråga om respondenten har upplevt någon form av phishing under sin tid hos företaget. Totalt 83 svar.

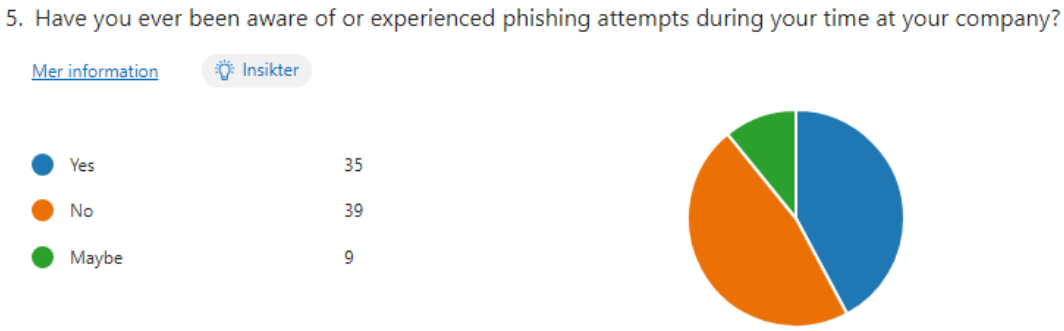

Fig. 4. Resultatdiagram fråga 5 enkät.

Fråga 6. Fråga om hur viktigt respondenten tror att uppmärksamhet på hot som dessa är på att förhindra phishing. Totalt 44 svar. 1 på skalan innebar "Inte alls effektivt" och 10 på skalan innebar "Extremt effektivt".

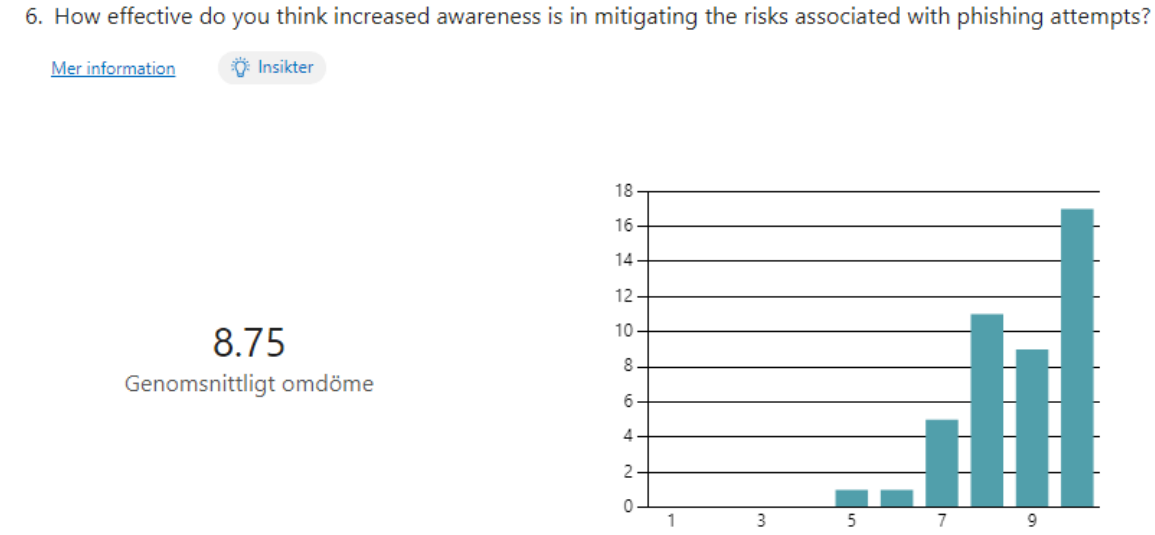

Fig. 5. Resultatdiagram fråga 6 enkät.

Fråga 7. Fråga om vilka typer av phishingförsök respondenten råkat ut för. Totalt 44 svar. Respondenten ombads klicka i Ja, Nej eller Kanske på samtliga former av attacker.

Email Phishing: (Yes: 90.9%) (Maybe: 2.3%) (No: 6.8%)

Printed QR codes or stickers: (Yes: 9.1%) (Maybe: 11.4%) (No: 79.5%)

Animated QR-codes: (Yes: 6.8%) (Maybe: 9.1%) (No: 84.1%)

Smishing (SMS Phishing): (Yes: 54.5%) (Maybe: 18.2%) (No: 27.3%)

Vishing (Voice Phishing): (Yes: 2.3%) (Maybe: 18.2%) (No: 79.5%)

Spear Phishing: (Yes: 36.4%) (Maybe: 13.6%) (No: 50%)

Real drive-by-phishing: (Yes: 25%) (Maybe: 15.9%) (No: 59.1%)

Other: (Yes: 13.6%) (Maybe: 34.1%) (No: 52.3%)

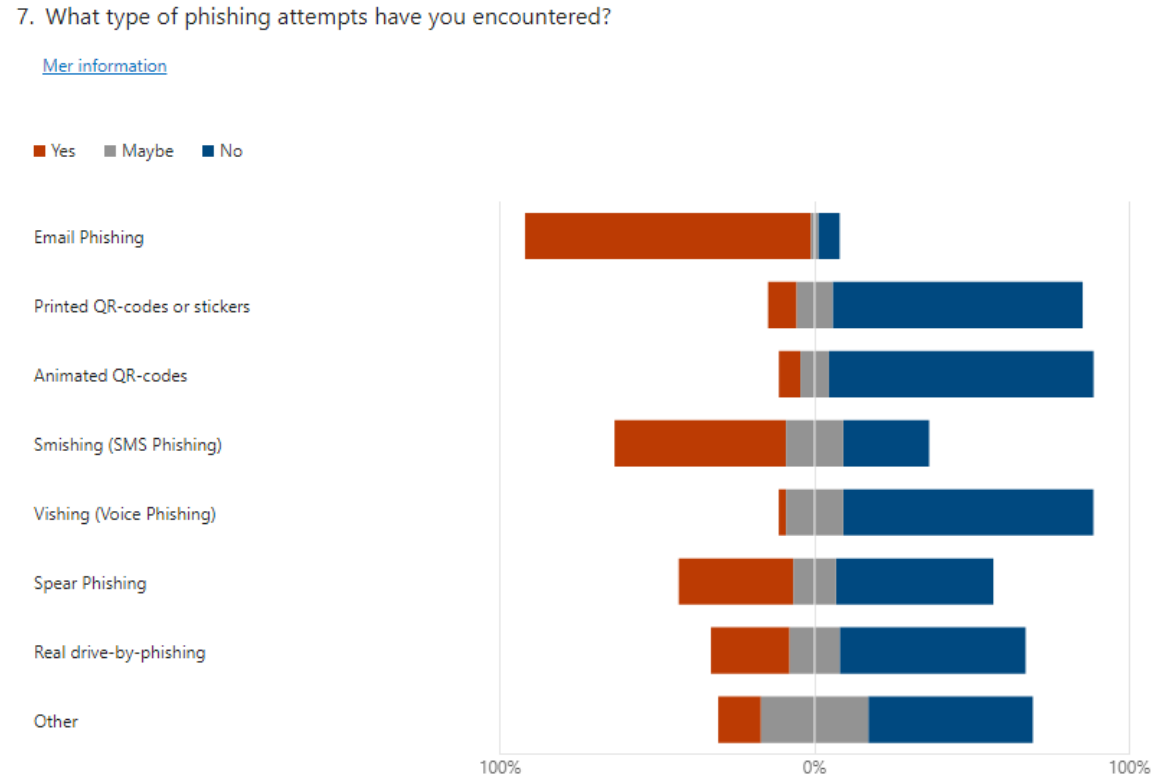

Fig. 6. Resultatdiagram över fråga 7 enkät.

Fråga 8. Fråga om respondenten har rapporterat ett phishingförsök i outlook till företages IT-säkerhets team. Totalt 44 svar.

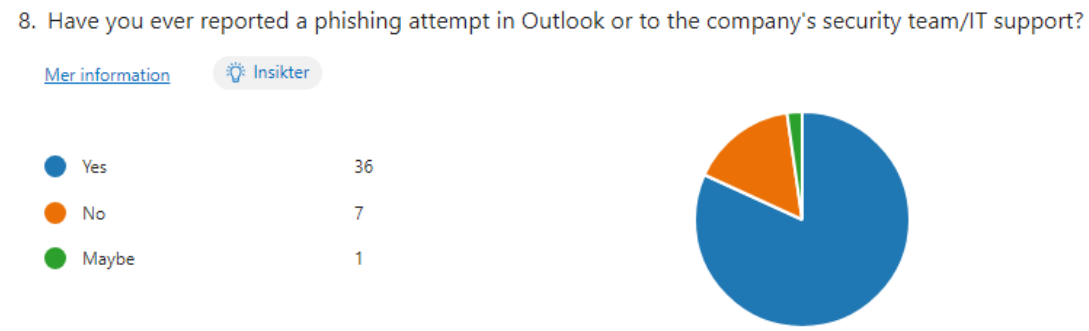

Fig. 7. Resultatdiagram över fråga 8 enkät.

Fråga 9. Fråga om respondenten känner sig självsäker i sin förmåga att upptäcka phishing attacker. Totalt 44 svar

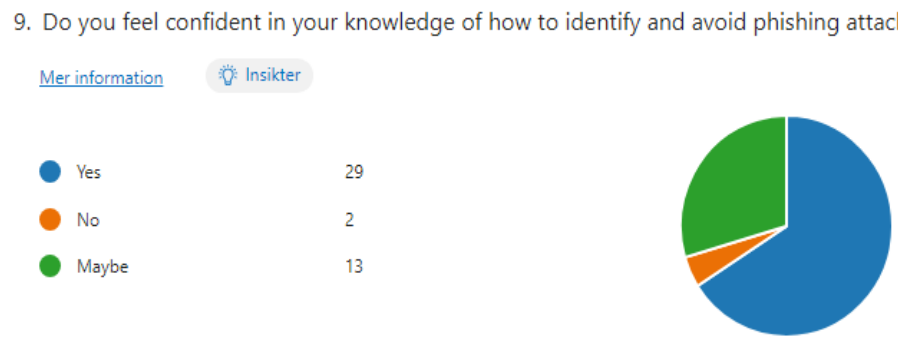

Fig. 8. Resultatdiagram över fråga 9 enkät.

Fråga 10. Fråga om respondenten tror att deras utbildning har påverkat deras förmåga att upptäcka phishing attacker. Totalt 44 svar

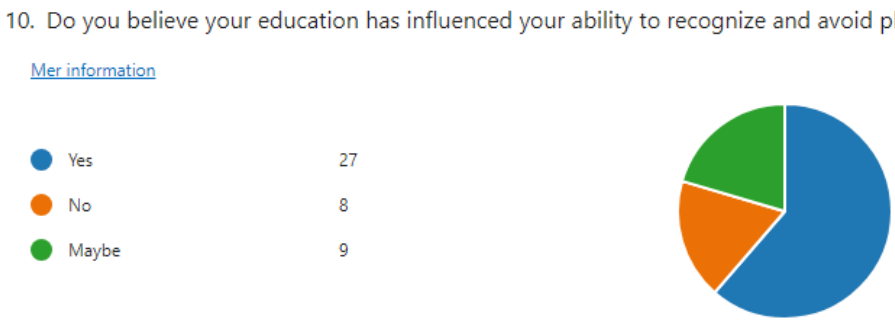

Fig. 9. Resultatdiagram över fråga 10 enkät.

Fråga 11. Fråga om hur viktigt respondenten tror att det är att man är vaksam och försiktig gentemot phishing-försök. Skala 1-10 där 1 står för "Inte alls viktigt" och 10 står för "Extremt viktigt" Totalt 44 svar

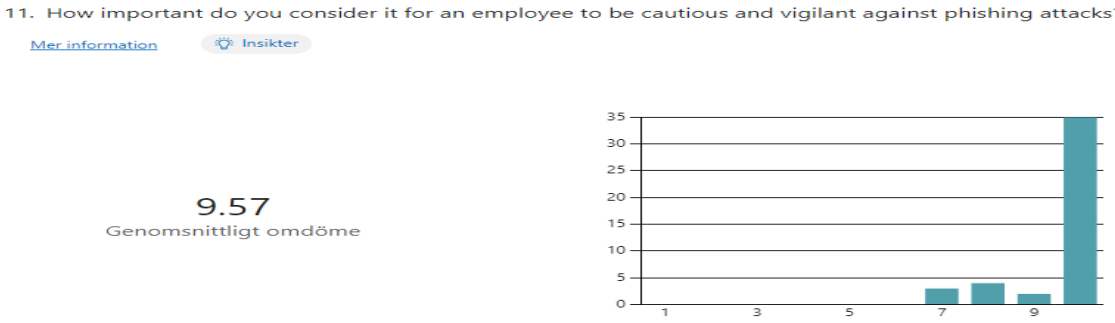

Fig. 10. Resultatdiagram över fråga 11 enkät

Fråga 12. Fråga om respondenten upplevt phishing försök av detta slag:

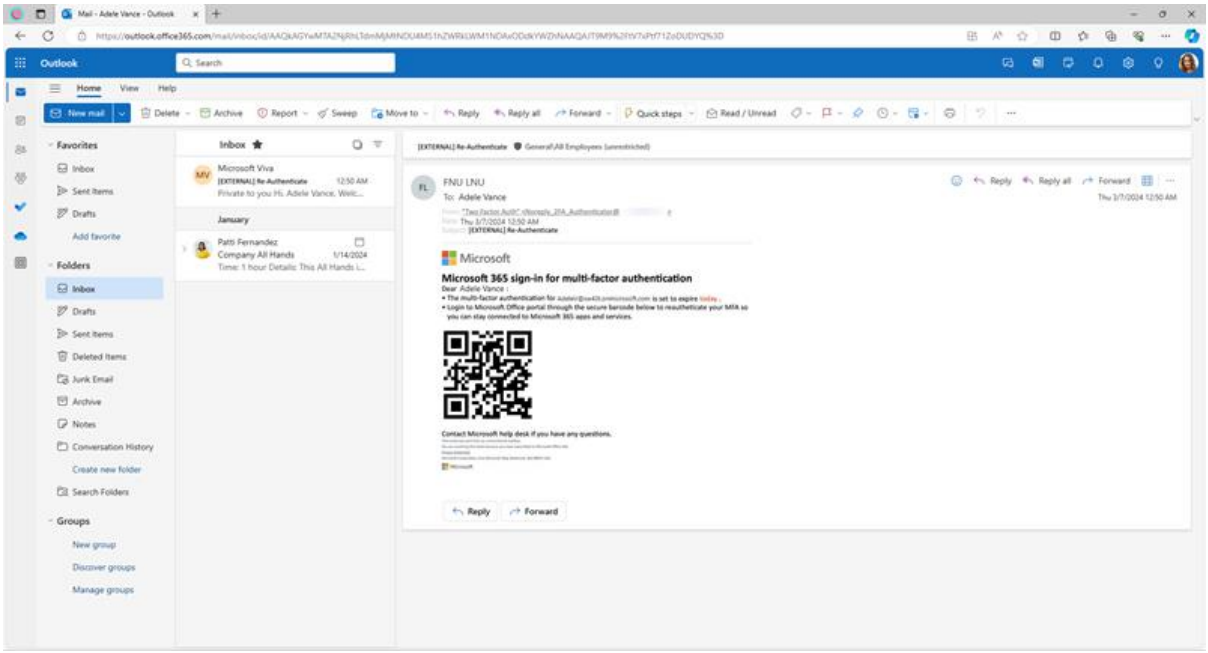

Fig. 11. En representation av ett simulerat phishingmail i den simulerade företagsmiljön, QR-koden leder till www.example.com.

Totalt 44 svar:

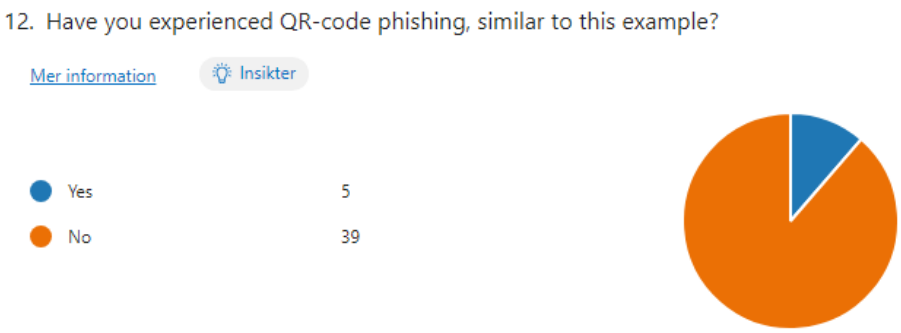

Fig. 12. Resultatdiagram över fråga 12 enkät.

Fråga 13. Fråga till de som svarade ja på fråga 12 om hur många gånger de råkat ut för sådana försök. Totalt 5 svar.

ID ↑	Namn	Svar	Språk
1	anonymous	5	Svenska
2	anonymous	1	Svenska
3	anonymous	3	Svenska
4	anonymous	2	English (United States)
5	anonymous	1	English (United States)

Fig. 13. Svar från respondenterna på fråga 13.

Fråga 14. Fråga om respondenten råkat ut för quishing i samma form som denna video: https://www.youtube.com/watch?v=1E7HDskAIHA&embeds_referring_euri=https%3A%2F%2Fforms.office.com%2F&source_ve_path=OTY3MTQ&feature=emb_imp_woyt

Totalt 44 svar:

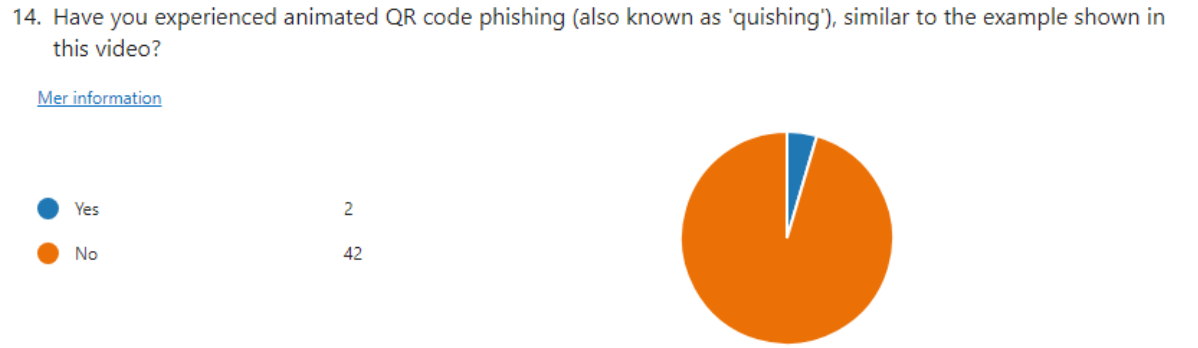

Fig. 14. Resultatdiagram över fråga 14 enkät.

Fråga 15. Fråga till de respondenter som svarade ja på fråga 14 om hur många gånger de upplevt attacker av denna form. Totalt 2 svar.

2 Svar

ID ↑	Namn	Svar	Språk
1	anonymous	5	Svenska
2	anonymous	1	Svenska

Fig. 15. Svar från respondenterna på fråga 15.

Fråga 16. Fråga till respondenterna om hur de bedömer risk-nivån av de hoten nämnda i fråga 12 samt fråga 14. Skala 1-10 där 1 stod för "Ingen risk" och 10 stod för "Extremt hög risk" Totalt 44 svar.

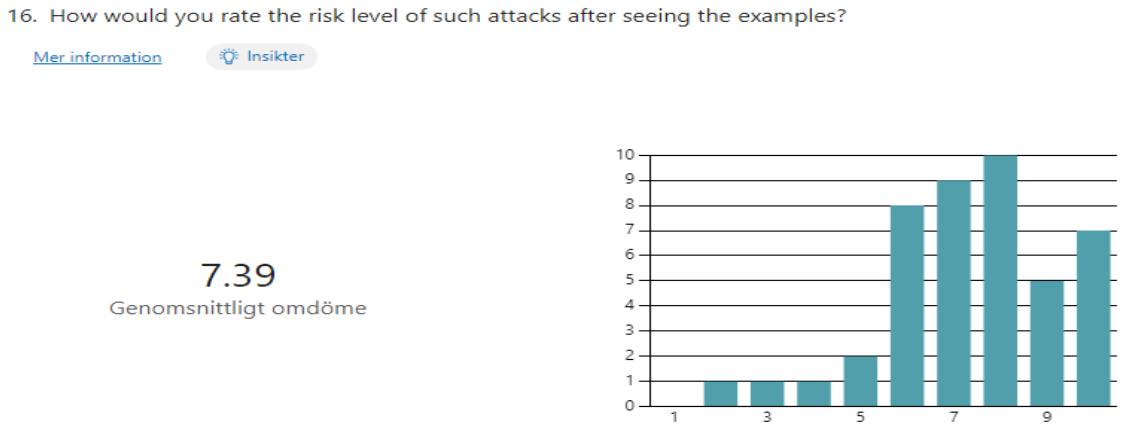

Fig. 16. Resultatdiagram över fråga 16 enkät.

Fråga 17. Fråga till respondenterna om hur svårt de tror att attacker som de visade i fråga 12 samt fråga 14 kan påverka hela företaget som helhet. Skala 1-10 där 1 stod för "Ingen risk" och 10 stod för "Extremt hög risk". Totalt 44 svar.

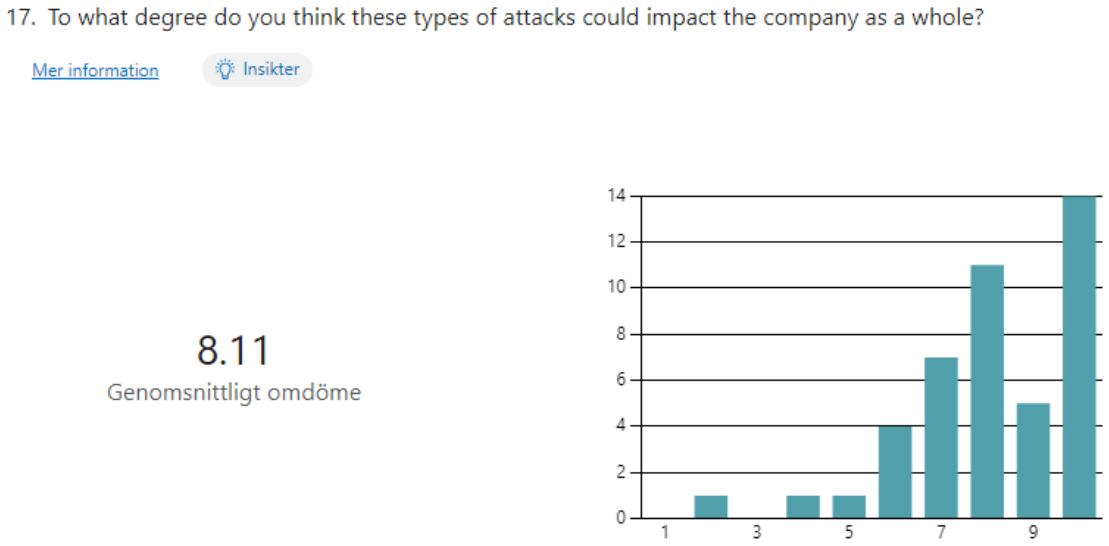

Fig. 17. Resultatdiagram över fråga 17 enkät.

Fråga 18. Fråga till respondenterna om hur nöjda de är med It säkerhetslösningarna som företaget står för. Skala 1-10 där 1 stod för "Mycket missnöjd" och 10 stod för "Extremt nöjd". Totalt 44 svar.

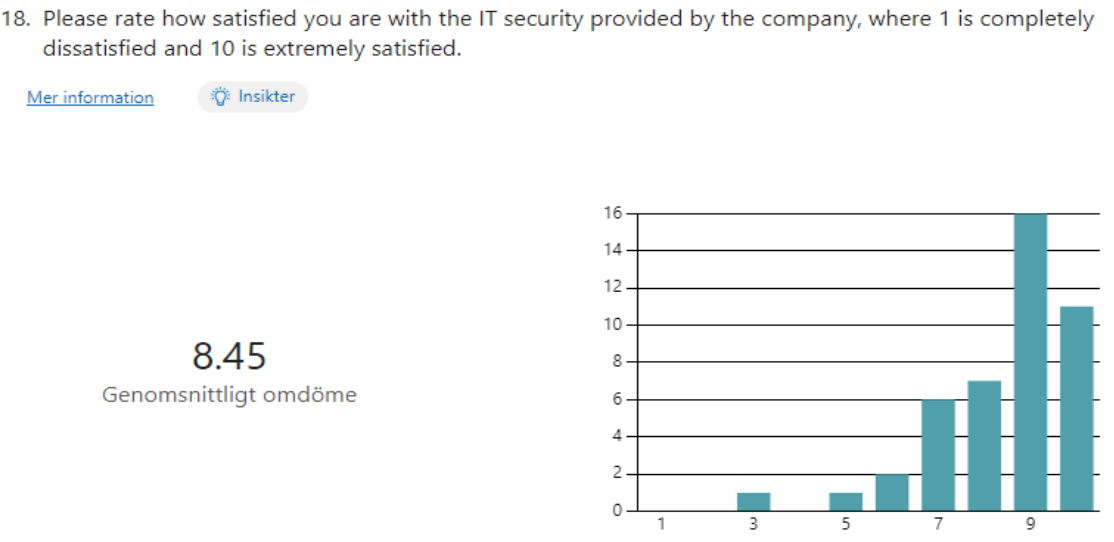

Fig. 18. Resultatdiagram över fråga 18 enkät.

Fråga 19. Fråga till respondenterna om hur bra de tycker företaget är på att stå för utbildning och resurser för att man som individ ska kunna motverka phishing attacker. Skala 1-10 där 1 stod för ”Mycket dåliga” och 10 stod för ”Exceptionellt bra”. Totalt 44 svar.

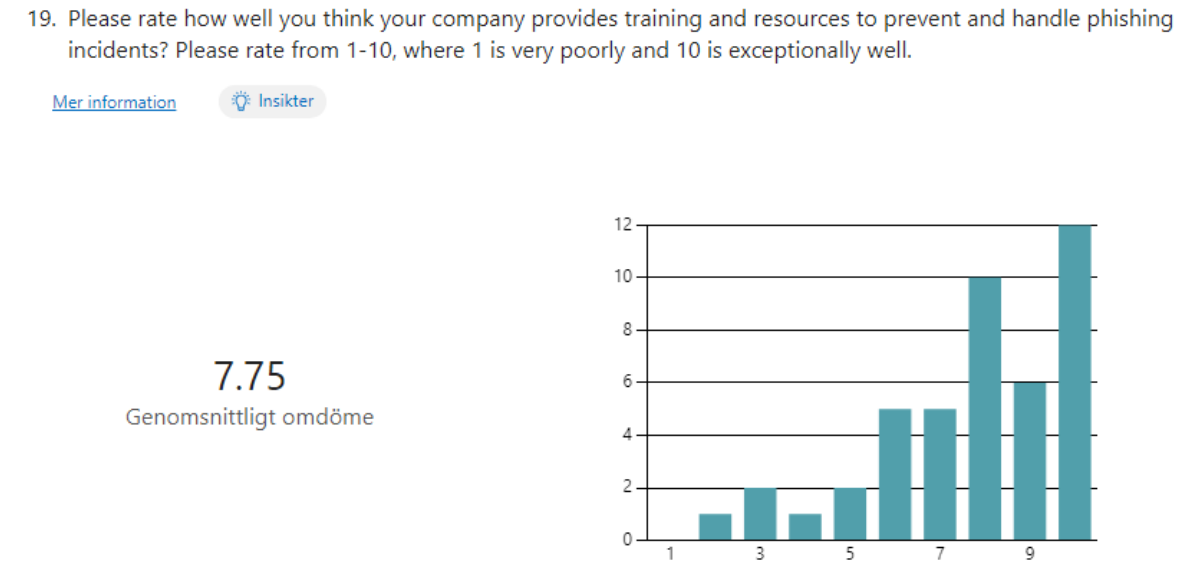

Fig. 19. Resultatdiagram över fråga 19 enkät.

Fråga 20. Fråga till respondenterna om hur uppskattade och stöttade de känner sig av företaget/företagsledningen. Skala 1-10 där 1 stod för “Inte stöttad alls” och 10 stod för “Extremt stöttad”. Totalt 44 svar.

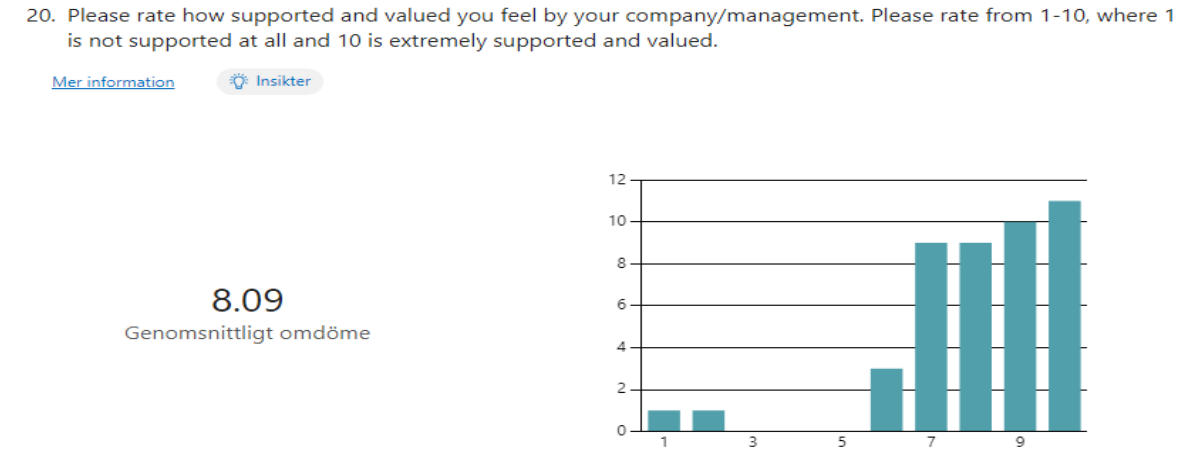

Fig. 20. Resultatdiagram över fråga 20 enkät.

Fråga 21. Fråga till respondenten om hur engagerade de känner sig för företagets framgångar och värderingar. Skala 1-10 där 1 stod för "Inte alls engagerad" och 10 stod för "Extremt engagerad". Totalt 44 svar.

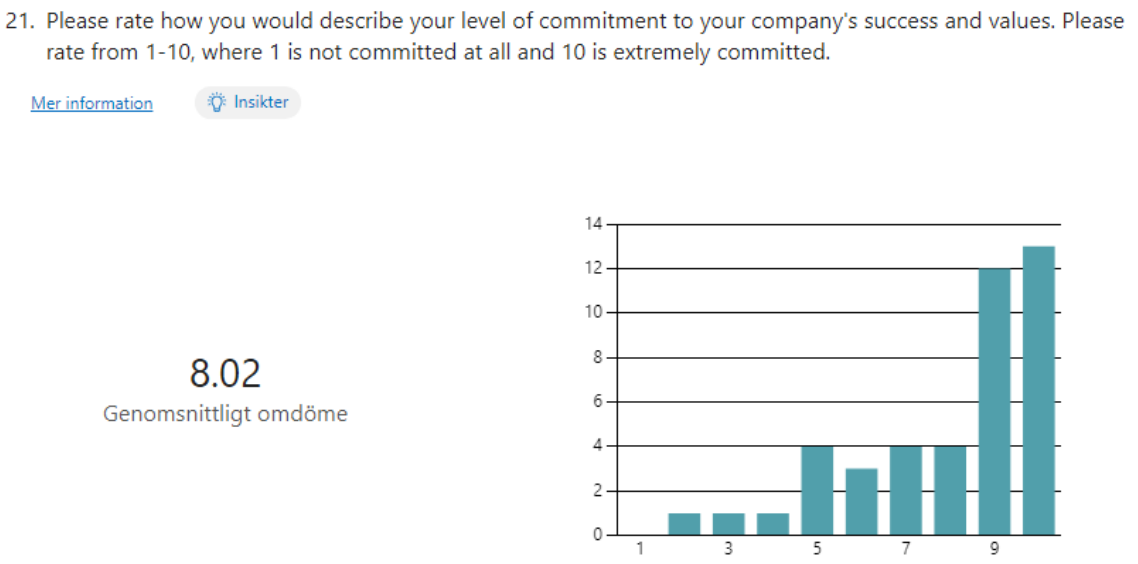

Fig. 21. Resultatdiagram över fråga 21 enkät.

Fråga 22. Fråga till respondenterna om de visste om eller använde någon app med inbyggt skydd mot quishing när de skulle skanna QR koder. Totalt 44 svar.

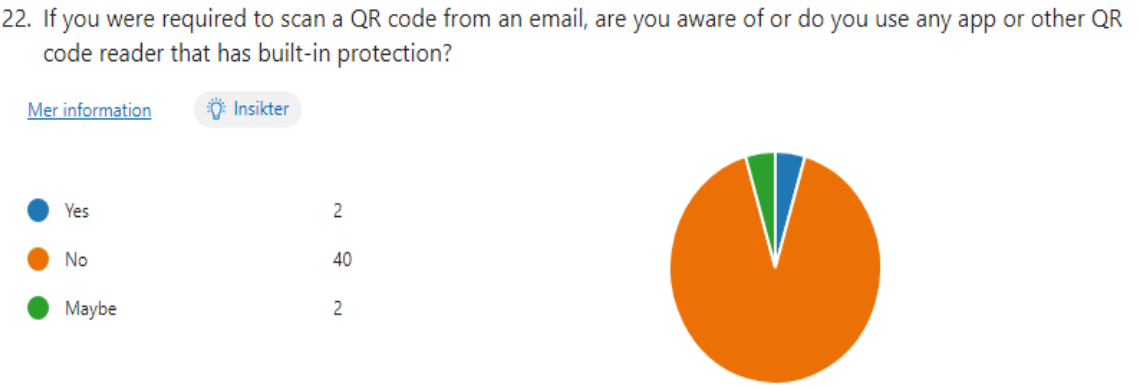

Fig. 22. Resultatdiagram över fråga 22 enkät.

Fråga 23. Fråga till de respondenter som svarade ja eller kanske på fråga 22 om vilken app de använde eller visste om. Totalt 3 svar.

23. What is the name of the app?

3 Svar

ID ↑	Namn	Svar	Språk
1	anonymous	————-	Svenska
2	anonymous	Vet ej	Svenska
3	anonymous	Camera (Samsung Built-in app) - shows the link of the QR and it relies on me pressing the link before re-directing me towards it.	English (United States)

Fig. 23. Svar från respondenter på fråga 23 enkät.

Fråga 24. Fråga om hur effektiv de respondenter som svarade ja eller kanske på fråga 22 upplevde att denna app med inbyggt skydd var. Skala 1-10 där 1 stod för "Inte alls effektiv" och 10 stod för "Extremt effektiv". Totalt 4 svar.

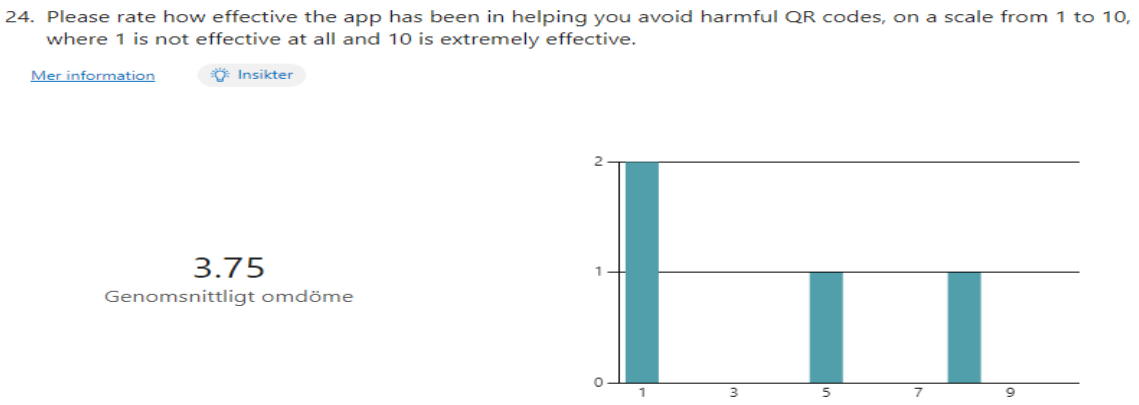

Fig. 24. Resultatdiagram över fråga 24 enkät.

Fråga 25. Fråga till respondenterna om de hade några förslag på hur företaget de jobbar på kan förbättra sin hantering och motverkning av phishing försök. Totalt 50 svar. Här finns det ett visst bortval av personer som inte gett ett fullständigt eller konkret svar. De svaren som exempelvis "?" kommer därav sorteras bort för att undvika förvirring vid läsande av listan, de svar som bara innehåller ordet "Nej" kommer även sorteras bort då det inte är relevant då frågan inte var obligatorisk att besvara. Detta görs även för att få ett bättre flöde i listan. Komplett lista på dessa svar som även inkluderar svar som anses felaktiga eller icke-komplette finns att läsa i Appendix B

1. Utbilda personal

2. Man kan berätta för personerna inom företaget att man ska vara försiktig med länkar osv.

3. Utbildning

4. Ja, fortsatta tydliga policyer och utbildningar för personalen oavsett vilken avdelning de sitter på.

6. Ja det gäller väl att främja en företagskultur som ständigt jobbar med att öka de anställdas medvetenhet om hot som dessa.

7. Vet inte, mitt företag är ganska bra på att hantera och motverka phishing

9. Utbilda i samtliga typer av phishing-attacker, det är stort fokus på phishing via mejl

10. Education

13. Limiterad användning av Mail samt telefon.

14. Skicka ännu fler mail antar jag.

15. My company already filters all emails sent to the company email, since i have not recieved or noticed any phising attempts at all, i would assume that the current methods are working very well, and can therefore not think of anything they could improve.

18. Utbildning

19. Genom återkommande utbildningar och även fejkade phising mail

21. Agera proaktivt, informera om riskerna och skapa medvetenhet genom att visa exempel på hur en attack kan gå till.

23. Nej det fungerar fint, de har bra koll och kontinuerliga ”tester” på alla oss anställda

28. Utbilda

29. Regelbunden utbildning av personalen. På min arbetsplats får vi ca varannan vecka frågor kring It-säkerhet som vi besvarar. Tar ca 5 min att fylla i. Därutöver testas vi regelbundet genom att falska mejl med länkar skickas.

32. Ha koll på medarbetare internet användning

34. Nej inte direkt. Kanske prata mer om det och inte bara via email-utbildningar.

36. Kontinuerlig utbildning

37. Anställa kompetent IT-personal med rätt förutsättningar för att motverka eller identifiera potentiella attacker.

39. Nej ev mera utbildning

40. Nej, fortsätter att arbetas kontinuerligt med detta. Både genom fejk meddelande och utbildning. Hellre ta bort ett mejl för mycket och få en påminnelse.

41. Genom kontinuerlig intern utbildning

42. Mer utbildning

43. Det är en bra fråga. Vi går igenom en hel del kurser för att känna igen inkräktare på våra mail och via fake sidor. Qr koder har vi inte gått igenom så mycket

45. Mer kontakt och bättre hantering. Större empati och förståelse

46. Yes, more training excercises and meetings for all kinds of Phishing attacks with a focus on specifically the QR Code, Animated QR Code and Voice Phishing attacks.

47. Short training are really good, keep it doing.

49. Continue with reminders and training

50. Run more simulations, spear-phishing specifically. Implement features in the employees inbox applications that makes it extremely clear what to look out for at all times. Give employees access to virtual environments to test links before actually using them. 1984-mode: Restrict access to html emails and that will be the end of it.

3.1.2 Kort sammanfattning av enkätsvaren

Här följer en kort sammanfattning av svaren på enkäten som användes under uppsatsen.

- Anställningstid och roller:

Medelvärdet för anställningstiden var 7,6 år, medan medianen var 3 år.

Respondenterna hade en mängd olika roller inom företaget, från Ekonomiassistent och IT-specialist till VD och Undersköterska.

- IT-utbildning:

Många respondenter hade någon form av IT-utbildning, antingen internt inom företaget eller formellt.

- Phishing-erfarenheter:

Cirka 53% av respondenterna hade råkat ut för phishing-försök under sin tid på företaget.

Email phishing var den vanligaste typen (90.9%), följt av smishing (54.5%) och spear phishing (36.4%).

- Rapportering och medvetenhet:

Hälften av de som hade upplevt phishing-försök hade rapporterat incidenter till företagets IT-säkerhetsteam.

Respondenterna kände sig relativt självsäkra i sin förmåga att upptäcka phishing-attacker, med ett genomsnittligt självförtroende på 7,5 på en skala från 1 till 10.

Utbildning ansågs ha en positiv effekt på förmågan att upptäcka phishing-attacker.

- Viktigheten av vaksamhet och riskbedömning:

Uppmärksamhet mot phishing ansågs vara mycket viktig, med ett medelvärde på 9,1 på en skala från 1 till 10.

Respondenterna bedömde risknivån för olika phishing-hot som hög, och de såg en betydande risk för företaget om sådana attacker lyckades.

- Nöjdhet med IT-säkerhetsåtgärder:

Generellt var respondenterna nöjda med företagets IT-säkerhetslösningar och utbildningar, men det fanns också förslag på förbättringar, såsom mer frekventa och varierade utbildningar och simuleringar av phishing-attacker.

- Förbättringsförslag:

Många respondenter föreslog ökad och kontinuerlig utbildning som den viktigaste åtgärden för att förbättra företagets hantering av phishing-försök.

Andra förslag inkluderade fler simuleringar av phishing-attacker och bättre intern kommunikation om säkerhetsrisker.

3.2 Säkerhetsverktygens effektivitet

I den genomförda experimentstudien utvärderades fyra olika säkerhetsverktyg, inklusive Microsoft Defender for Office (MDO), för verktygens förmåga att identifiera och blockera skadliga QR-koder och URL:er i klartext som förekom i aktuella phishing-attacker. Nedan presenteras de kvantitativa resultaten från experimentet, uppdelat på de olika verktygen och testtyperna, den fullständiga insamlade data återfinns också i Appendix D, se figur 58.

3.2.1 Microsoft Defender for Office (MDO)

Microsoft Defender for Office (MDO) testades i tre olika scenarier: detektion av skadliga URL:er i klartext, statiska QR-bilder, och animerade QR-bilder (se Figur 25). Resultaten presenteras separat:

Blockerade URL:er i klartext

Sann Positiv: Åtta

Falskt Negativ: Åtta

Sann Negativ: 16

Falskt Positiv: Noll

Noggrannhet: 75%

Känslighet: 50%

Specificitet: 100%

Blockerade statiska QR-bilder

Sann Positiv: Åtta

Falskt Negativ: Åtta

Sann Negativ: 16

Falskt Positivt: 0

Noggrannhet: 75%

Känslighet: 50%

Specificitet: 100%

Blockerade QR-animationer

Sann Positiv: Noll

Falskt Negativ: 16

Sann Negativ: 16

Falskt Positiv: Noll

Noggrannhet: 50%

Känslighet: 0%

Specificitet: 100%

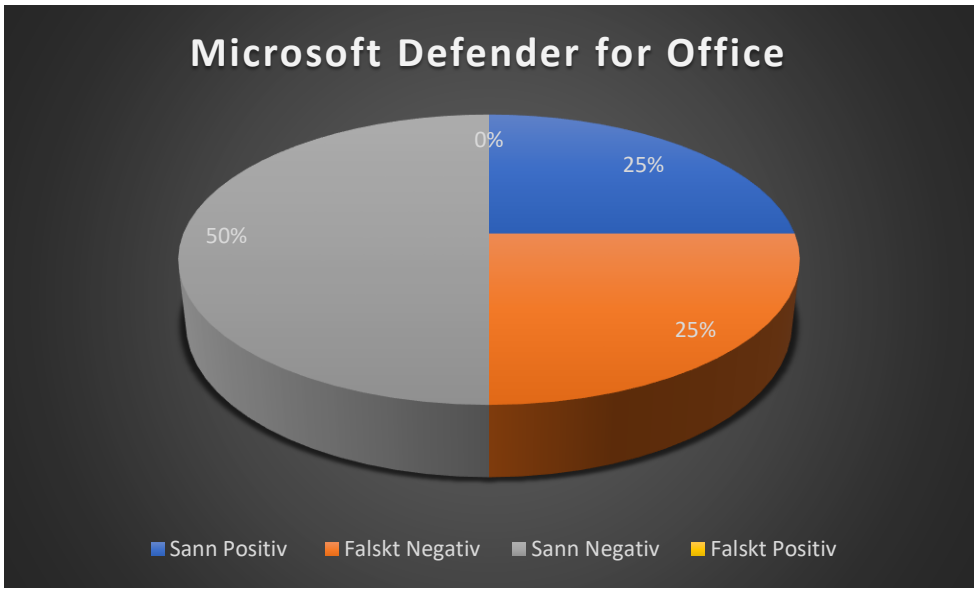

Fig. 25. Cirkeldiagram över blockerade URL:er i MDO.

3.2.2 Andra säkerhetsvektyg

Eset Premiums effektivitet mot kontrollerade länkar i QR-koder som förekom i webbläsaren Edge (se Figur 26).

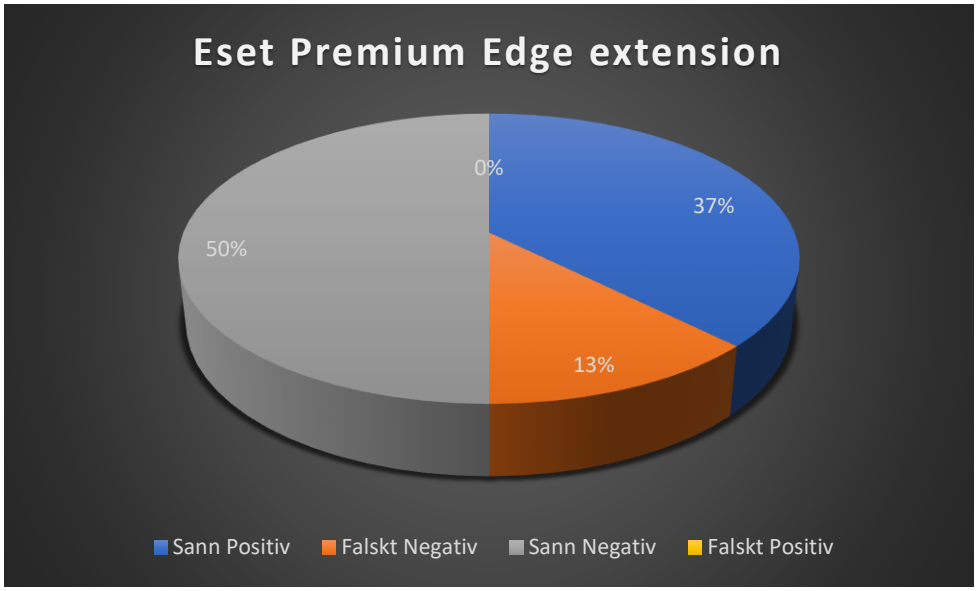

Fig. 26. Cirkeldiagram över blockerade URL:er med Eset Premium Edge extension.

Sann Positiv: 12

Falskt Negativ: Fyra

Sann Negativ: 16

Falskt Positiv: Noll

Noggrannhet: 87.5%

Känslighet: 75%

Specificitet: 100%

Trend Micro QR Scanner

Resultaten för Trend Micro QR scanner indikerar en fullständig detektionsförmåga bland de skadliga quishing länkarna som valdes ut för detta experiment (se Figur 27).

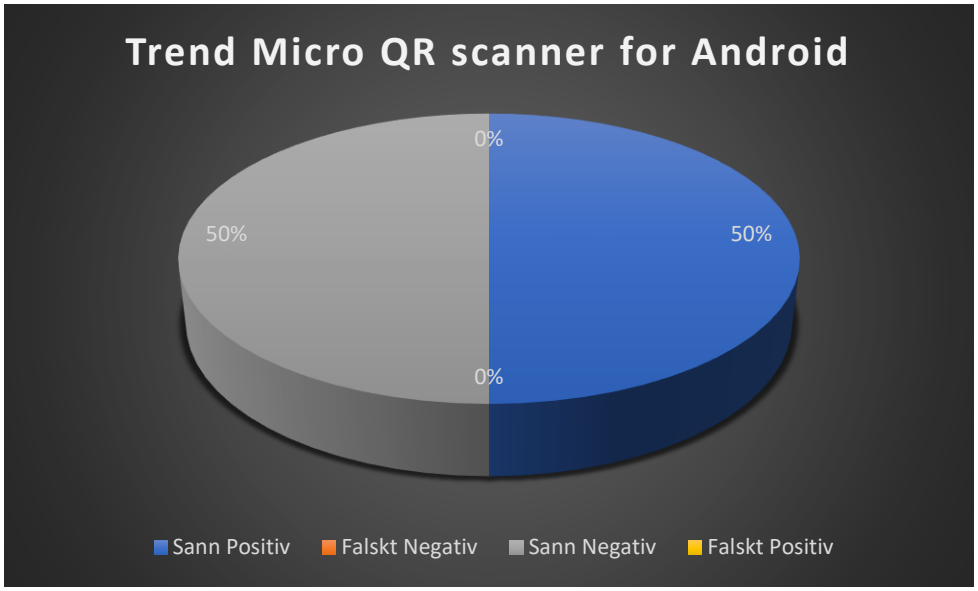

Fig. 27. Cirkeldiagram över blockerade URL:er med appen Trend Micro QR scanner.

Sann Positiv: 16

Falskt Negativ: Noll

Sann Negativ: 16

Falskt Positiv: Noll

Noggrannhet: 100%

Känslighet: 100%

Specificitet: 100%

Kaspersky Appen för Android visade följande prestanda i experimentet (se Figur 28).

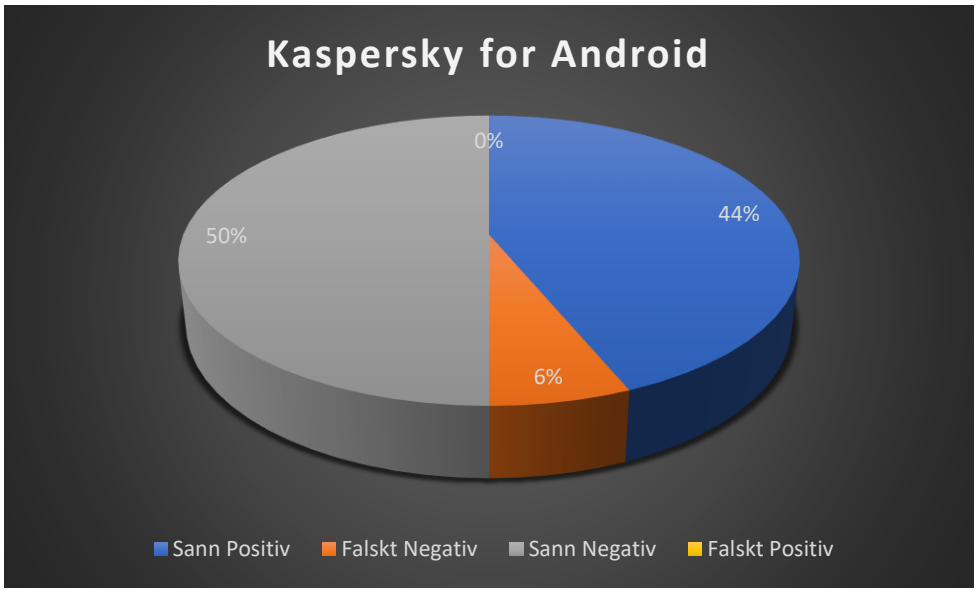

Fig. 28. Cirkeldiagram över blockerade URL:er för appen Kaspersky for Android.

Sann Positiv: 14

Falskt Negativ: Två

Sann Negativ: 16

Falskt Positiv: Noll

Noggrannhet: 93.75%

Känslighet: 87.5%

Specificitet: 100%

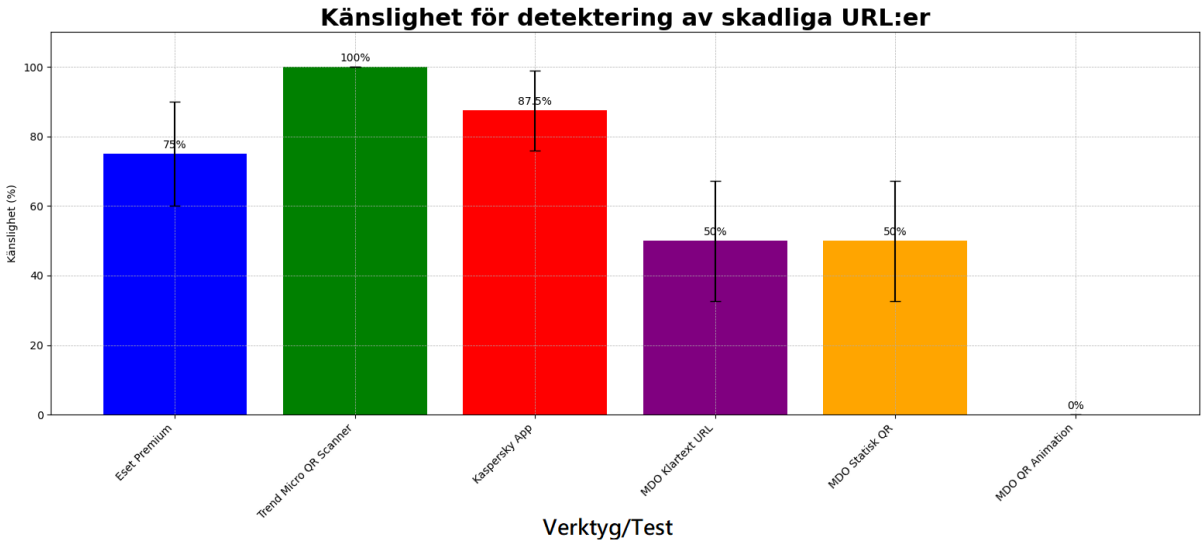

Fig. 29. De olika verktygens känslighet att detektera skadliga URL:er. Det syns även error bars med konfidensintervall på 95%.

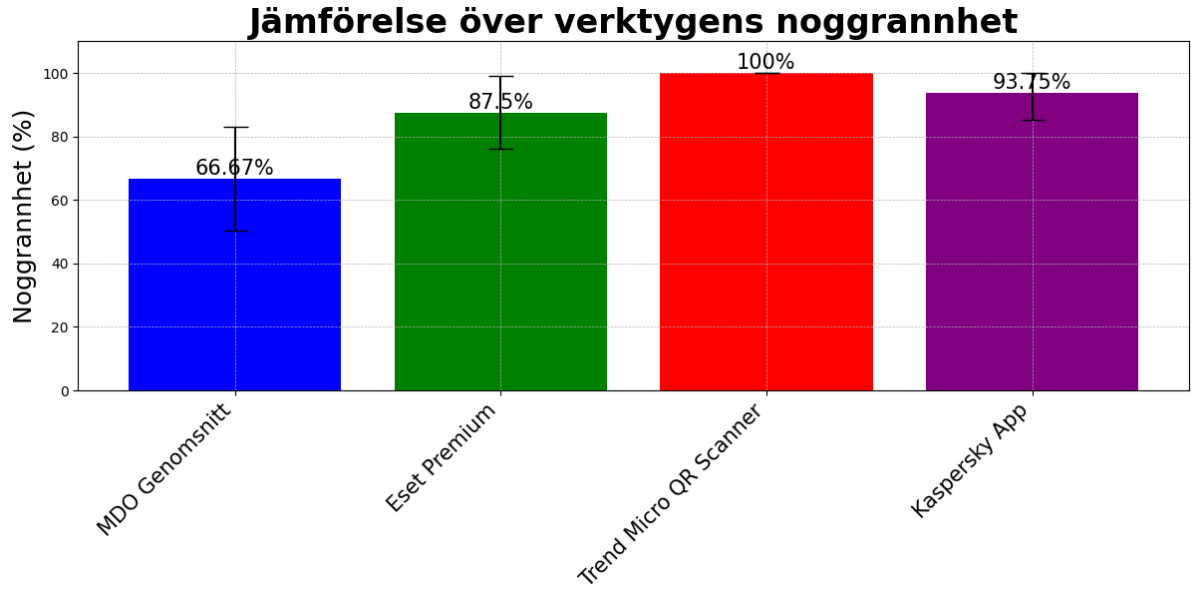

Fig. 30. Diagrammet visar noggrannheten för Microsoft Defender for Office (MDO), vilket är ett genomsnitt över tre olika tester, jämfört med Eset Premium, Trend Micro QR Scanner och Kaspersky App. Konfidensintervallen är beräknade med 95% säkerhet.

3.2.3 Sammanfattning över resultaten i experimentet

Resultaten från experimentstudien visar en variation i prestanda mellan de olika säkerhetsverktygen. Microsoft Defender for Office (MDO) uppvisade varierande effektivitet, med en märkbar skillnad i dess förmåga att detektera skadliga URL:er i klartext och statiska QR-bilder jämfört med animerade QR-bilder (se Figur 29). Eset Premium, Trend Micro QR Scanner, och Kaspersky App visade övergripande en högre effektivitet, med Trend Micro QR Scanner som identifiera alla testade skadliga länkar utan några falskt positiva resultat (se Figur 30).

3.3 Attack simulation training utförd av MSSP

Det utfördes en AST under tre olika perioder för att utvärdera hur personalen hanterar skadliga e-postmeddelanden. Resultaten över den genomförda AST som illustreras i Fig. 31, visar antal deltagare som kompromettерades eller som rapporterade meddelanden som phishing. I januari klickade en större andel på skadliga länkar och i mars ökade andelen rapporterade meddelanden däremot i april minskade denna siffra igen.

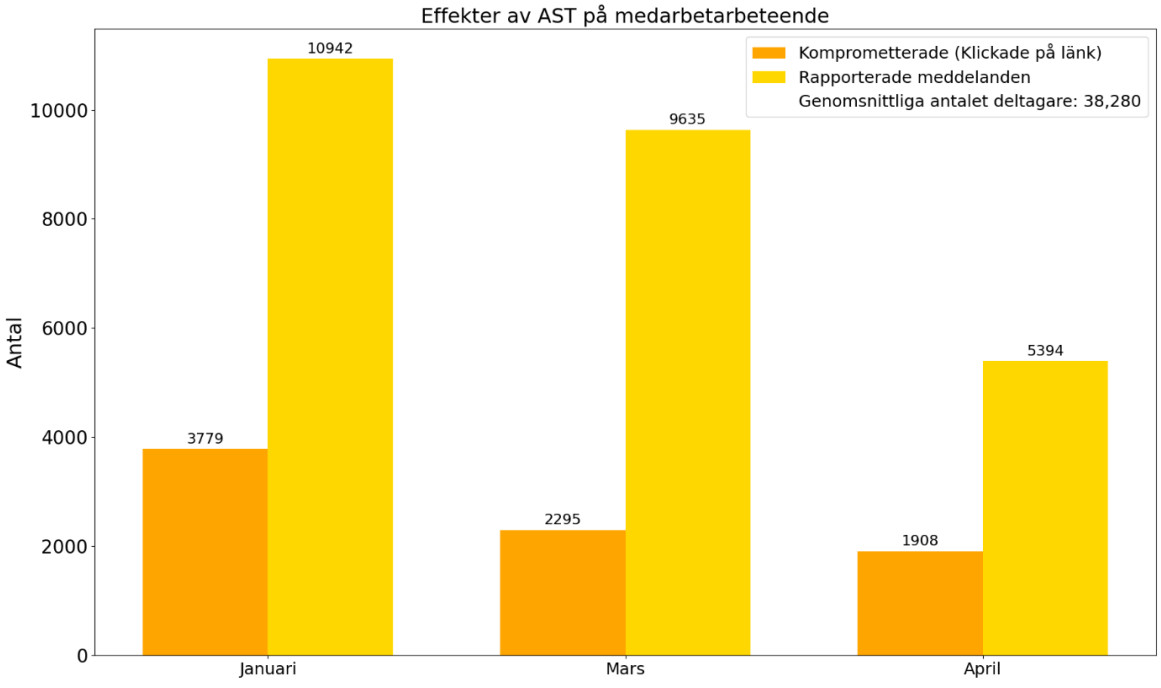

Fig. Fig 31. Diagrammet visar resultatet av de olika AST utförda av MSSP.

1 Januari - 7 Januari
Typ av simulering: Drive-by-simulering som efterliknar en intern process för uppdatering av enheter.
Kompromettерade (Klickade på länk): 9.62%
Rapporterade meddelanden: 27.88%
Lästa meddelanden: 63.66%
Raderade meddelanden: 36.42%
Antal deltagare: 39,279

7 Mars - 14 Mars
Typ av simulering: Drive-by-simulering som imiterar en intern kommunikationsapp och varnar om otillåten inloggning.
Kompromitterade (Klickade på länk): 6.66%
Rapporterade meddelanden: 27.97%
Lästa meddelanden: 53.73%
Raderade meddelanden: 42.82%
Antal deltagare: 34,447

1 April - 7 April
Typ av simulering: Drive-by-simulering som efterliknar en intern applikation som kräver licensuppdatering.
Kompromitterade (Klickade på länk): 4.64%
Rapporterade meddelanden: 13.12%
Lästa meddelanden: 54.68%
Raderade meddelanden: 30.21%
Antal deltagare: 41,113

4. Diskussion

Denna studie strävar efter att undersöka huruvida de forskningsresultat som presenterats av N. Beu et al., gällande företagssimuleringar följda av enkäter, är trovärdiga och innefattar nyare phishinghot som quishing. Detta inkluderar att verifiera och jämföra dessa resultat med det som framkommit i denna studie samt att utforska möjligheten att identifiera nya mönster som inte tidigare observerats. Deras studie antyder att anställda med kortare anställningstid, samt de som uppvisar lägre nivåer av tillfredsställelse och lojalitet mot företaget, tenderar att bete sig osäkrare i simuleringarna. Vidare visar deras resultat att individer med nyare anställning och mindre nöjda anställda är särskilt sårbara för phishingförsök och skulle ha störst nytta av specifikt riktade utbildningar i cybersäkerhet samtidigt som de menar att det är osannolikt att utbildning och träning skulle vara effektivt om en anställd förlitar sig på ett verktyg och skulle därmed inte känna något ansvar för företagets säkerhet [15]. studiens enkätundersökning indikerar att det finns ett behov av att stärka företagskulturen och tillfredsställelsen för personalen för att öka rapporteringsfrekvensen och därmed förbättra det allmänna säkerhetsbeteendet. Detta är i linje med Beu et al. men att det skulle vara osannolikt att utbildning och att personalen skulle förlitar sig enbart på säkerhetsverktyget är inte fallet och går inte att styrka med studiens data. Tvärt om kan det ses vissa indikationer i uppsatsens undersökning att den utförda ASTn faktiskt hjälper. Denna analys ger en första fingervisning men för att ytterligare bekräfta dessa indikationer, rekommenderas att det utförs djupare statistiska analyser med en större datamängd och respondenter i enkätundersökningar för att öka validiteten [21].

Omfattningen och bredden av studien med både enkätstudie, inblick i ett företags AST och en undersökning av säkerhetsvektyg vill undersöka alla realistiska delar som kan påverka ett företags resiliens mot den ökade mängden och mångfalden av phishing.

Ett val gjordes att dela upp diskussionen i tre delar för att underlätta analysen av de metoderna som använts. De delar som diskussionen är uppdelad i är Enkätdiskussion, AST-diskussion samt Experimentdiskussion. Där går uppsatsen in på detaljnivå i samtliga metoder för att analysera och hämta ut information som bedöms vara relevant för att besvara de valda frågeställningarna samt den information som anses främja uppsatsens syfte.

4.1 Enkätdiskussion

Efter en noggrann granskning och analys av resultaten i enkäten som skickades ut till de anställda så är det viktigt att börja med att poängtera faktumet att de främsta formerna av phishing fortfarande är email phishing och sms phishing, se figur 6. Detta är något som stämmer överens med statistiken som förts över olika phishing attacker där Email phishing ligger som etta på listorna över de vanligaste phishingteknikerna [11], [24], [25]. Detta medan formerna av Quishing, både i statiskt format och animerat format än inte visat sig vara vanligt förekommande hos de respondenter som besvarade studiens enkät. Det framkommer dock att, även om inte quishingen har varit ett vanligt förekommande fenomen hos studiens urvalsgrupp så ser studiens respondenter allvarligt på hot som dessa. Efter analys av figur 16 och figur 17 så kan det ses att den allmänna uppfattningen hos de som svarat är att risknivån hos hot som dessa ligger mellan 7-9 på en 10 gradig skala där 1 betydde “Ingen risk” och 10 “Extrem risk”.

Vad tolkningen av detta kan ge är då att respondenterna såg att det fanns höga risker med en främmande phishing-teknik som de ännu inte varit utsatta för.

Ett annat viktigt faktum när granskning av de anställdas bakomliggande utbildning och om de genomgått någon utbildning inom IT så ses det att en andel på 26 av 83 respondenter svarat att de inte genomgått någon utbildning alls när det kommer till IT, se figur 3. Detta är en oroande siffra både för individerna i fråga samt företagen de jobbar på. Om en så stor andel på 31% i denna undersökning inte genomgått en utbildning så kommer dessa individer förmodligen ha svårare att upptäcka tecken på phishing-attacker och kan därför vara ett direkt hot mot individens och företagets integritet. Trots avsaknaden på relevant IT utbildning så visar andra siffor på att även dessa respondenter lägger stor vikt vid individens ansvar i att vara med och motverka och förhindra phishing, se figur 5. Den visar på en allmän uppfattning om att individens uppmärksamhet och försiktighet spelar en vital del i att motverka dessa risker.

Vidare så kan det ses att på enkätens sista fråga där respondenten ombes ge förslag på vad företaget kan göra för att förbättra sin hantering när det kommer till phishinghot så kan en se en del olika förslag. Detta trots att den allmänna uppfattningen om hur nöjda respondenterna var med sitt företags IT-säkerhet och hur bra de tyckte att deras företag var på att tilldela de resurser och den kunskap som krävs för att medarbetarna ska kunna vara med och bidra till motverkan av phishing-försöken. Där låg medelvärdet av resultaten på 7.75 på fråga 18 och 8.45 på fråga 19, se figur 18 & 19. Detta tyder på att de respondenter som svarat på denna fråga generellt sätt är ganska nöjda när det kommer till företagets hantering av phishing-hot.

Kollas då svaren på fråga 25, se figur 57. Så kan det ses främst att de anställda föreslår mer intern utbildning inom företaget, det framkommer dock att många av respondenterna redan har bra utbildning på hot som dessa men att det främst handlar om email phishing. De föreslår då att fortsätta med kontinuerlig utbildning men att företaget även ska implementera flera former av phishing-simuleringar såsom att inkludera former av quishing eller vishing då det kan bli ett mer vanligt förekommande fenomen i framtiden i takt med att bedragarnas taktiker ständigt utvecklas i tid med att företagen lärt sig anpassa sig till deras äldre metoder. Email phishing har uppenbarligen blivit väl uppmärksammat av företagen som studiens respondenter jobbar på och då har företagen implementerat åtgärder som att utbilda sin personal mot just dessa hot. Detta kommer dock även bedragarna lägga märke till och kommer i sin tur utveckla sina metoder för att gå runt de anställdas kunskap.

Quishing utnyttjar QR-koder för att dirigera användare till skadliga webbplatser eller för att automatiskt initiera skadliga nedladdningar, vilket kan leda till obehörig dataåtkomst eller kompromettering av användarens enhet med virus. Zero Trust-arkitekturen kan effektivt begränsa dessa hot genom att eliminera möjligheten till lateral rörelse inom nätverket vilket denna metod kan en angripare möjlighet att fritt röra sig och sprida skadlig kod efter det initiala intrånget genom phishing [5], [6].

Som respondent med ID 50 i enkätstudien föreslog, kan en implementering av virtuella miljöer där anställda kontrollerar länkar innan de används, samt restriktioner mot HTML-e-post, erbjuder ytterligare skydd mot quishing och andra relaterade attacker. Forskare på Zscaler ThreatLabz rekommenderar också implementering av SSL-inspektion i full skala och

webbläsarisolering som delar av en Zero Trust-modell för att förhindra kompromettering genom phishing, särskilt när komplexiteten av attackerna kommer att öka markant med hjälp av olika maskininlärnings tjänster som chatGPT ökar också behovet av red teaming och andra mindre konventionella metoder för att stävja framtida attacker [5], [9], [10]. Som Jillepalli et al. (2018) påvisar, kan implementeringen av minsta privilegium principen på applikationsnivå, specifikt inom webbläsarkonfigurationer, avsevärt förstärka ett företags försvar mot cyberhot. Genom att begränsa användarnas behörigheter till enbart det nödvändigaste, minskar möjligheterna för skadliga aktörer att utnyttja quishing-attacker till att infiltrera företagsnätverk [7].

Denna information tillsammans med information kring experimentet samt attacksimulationen ger en bra uppfattning för att besvara första och tredje frågeställningarna:

1. Vilka strategier och metoder är mest effektiva för att höja medarbetares medvetenhet och engagemang i att förebygga quishing och andra relaterade cyberhot?

3. Hur kan en organisations säkerhetsåtgärder utformas för att effektivt hantera det växande hotet av quishing med hänsyn till potentiella konsekvenser för företagssäkerhet?

När rapporten vill besvara den första frågeställning utifrån vad respondenterna upplevde i enkäten och vad de svarade så har detta arbete kommit fram till strategier som av respondenterna anses vara de mest effektiva i att förebygga quishing och andra relaterade cyberhot. Denna lista med strategier sammanfogat med informationen från de andra metoder finner ni i experimentdiskussionen samt i slutsatsen.

4.2 AST-diskussion

Under det första kvartalet 2024 gav Attack Simulation Training (AST) en grundlig insikt i hur specifika designelement och indikatorer i phishing-simuleringar påverkar medarbetarnas förmåga att identifiera och hantera säkerhetshot. Genom att noggrant jämföra de olika simuleringarnas resultat framträdde klara mönster i deltagarnas beteenden, vilket gav värdefull information om vilka aspekter av simuleringarna som hade störst effekt.

Varje simulering innehöll designade indikatorer som brådskande meddelanden, domänförfalskning och URL-länkningar, som alla är avsedda att öka övertygelsen om ett legitimt meddelande. Brådskande meddelanden, som var särskilt framträdande i simuleringarna i januari och april, skapade en känsla av akut behov att agera, vilket ofta leder till att användare bortser från andra varningssignaler och ökar sannolikheten för att hotaktören ska lura offret till att klicka [8]. Dessa meddelanden bidrog till de högsta kompromettеringsnivåerna under dessa månader, 9.62% i januari och en minskning till 4.64% i april, vilket visar på en förbättring i medarbetarnas förmåga att kritiskt granska sådana uppmaningar. Domänförfalskning användes konsekvent i alla tester för att efterlikna legitima avsändare, vilket bidrog till att upprätthålla en viss autenticitet över phishingförsöken. Trots detta uppvisar de varierande handlingarna gällande URL-länkningar att deltagarnas

uppmärksamhet på sådana detaljer ökade över tid, sannolikt till följd av upprepad exponering för attacksimulationerna eller en minskning av deltagarnas nyfikenhet [12].

Med den annorlunda simulationsdesignen i mars som liknade en intern kommunikationsapp, observerades en förbättring med en kompromettеringsnivå på 6.66% och en rapporteringsnivå på 27.97%. Denna simulationsdesign var mindre brådskande och saknade några av de mer akuta indikatorerna, vilket kan ha bidragit till en mer genomtänkt handling av deltagarna.

April månads simulering introducerade unika indikatorer relaterade till interna applikationer, vilket antagligen minskade misstänksamheten och ökade acceptansen för de simulerade meddelandena. Trots en markant minskning av kompromettеringsnivån noterades även en avtagande rapporteringsfrekvens, vilket kan indikera en ökad tillit till eller vana vid simulationerna.

Detaljerna i dessa simuleringar visar en tydlig trend av minskade kompromettеringsnivåer från januari till april, samtidigt som rapporteringen av misstänkta meddelanden varierade, med en topp i mars följt av en nedgång i april (se figur 31). Denna förändring i rapporteringsbeteendet kan spegla hur olika designegenskaper i de simulerade phishingförsöken var mer eller mindre övertygande, vilket påverkade mottagarnas benägenhet att rapportera eller radera meddelanden. Likadant kan simulationen i april, med de unika och mer sällsynta applikationerna avskräcka mottagaren från att radera meddelandet helt och därmed behöva riskera eller försvåra en återställning av de interna applikationerna, även om interaktionen var lägre med simuleringsobjektet jämfört med tidigare tester. Deltagandet är dessutom mycket högre april månad, så en kan inte rakt av jämföra med föregående månad när det var som lägst antal deltagare i jämförelsen mellan januari och april månad med en lägre benägenhet att radera meddelandet men en halvering av antalet anställda som klickade på själva länken. Särskilt när det är ett brådskande meddelande och handlar om uppdateringar ökar detta sannolikheten att hotaktören lyckas [1], [2], [17]. Dessa observationer understryker vikten av att fortsätta anpassa och variera säkerhetssimuleringarna för att hålla medarbetarnas vaksamhet på en hög nivå och för att säkerställa att de är förberedda på en rad olika phishing-taktiker.

Microsoft skulle snabba på appliceringen av att utföra okonventionella attack simulationstester, med just quishing för de anställda både när det kommer till QR-koder levererade med e-post och QR-koder i det vilda, där vissa bedragare klistrar över befintliga koder med en ny QR-kod som leder någon helt annanstans. Även om det förnuvarande finns två läromoduler, saknas det AST-moduler som kan sättas i gång av företagets ansvariga för att utföra simulationerna och skapa en större medvetenhet. Detta betonar en viktig lucka i Microsofts nuvarande utbildningsresurser, vilket är anmärkningsvärt eftersom Microsoft själva lyfter fram betydelsen av att träna användare för att bli mer motståndskraftiga mot quishing-attacker via QR-koder. Enligt artikeln i Microsoft Tech Community, bör utbildningen inte bara fokusera på att känna igen skadliga QR-koder utan också stärka de anställdas förmåga att säkert interagera med QR-koder i alla miljöer, vilket inkluderar att verifiera autenticiteten av QR-koder innan webbplatsen besöks [20].

4.3 Experimentdiskussion

Resultaten från experimentstudien ger insikt i effektiviteten hos olika säkerhetsverktyg för att identifiera och blockera skadliga QR-koder och phishing-länkar, vilket är av betydelse för att bekämpa cyberhot och skydda användare mot potentiella säkerhetsrisker. Vidare granskning av resultaten avslöjar både styrkor och begränsningar hos de testade verktygen och ger vägledning för framtida förbättringar och forskning inom detta breda och ständigt föränderliga område.

Stapeldiagrammen i figur 29 ger en tydlig uppfattning av vad studiens undersökning representerar och den statistiska säkerheten bakom mätningarna.

Figur 30 förmedlar tydligt att MDO:s värde är ett genomsnitt och specificerar att konfidensintervallen gäller för samtliga presenterade verktyg, vilket är relevant för att understryka mätningarnas osäkerhetsmarginaler i den experimentella undersökningen.

En av de mest anmärkningsvärda observationerna är den varierande effektiviteten hos Microsoft Defender for Office (MDO) i att detektera olika typer av skadliga QR-koder och phishing-länkar. Trots dess förmåga att effektivt blockera skadliga URL:er i klartext och statiska QR-bilder samt en hög detektionsförmåga av nya hot [18], visade MDO en betydligt lägre förmåga att hantera animerade QR-bilder, med en noggrannhet på endast 50%. Detta indikerar en potentiell sårbarhet i MDO:s detektionsalgoritmer när det gäller att hantera dynamiskt innehåll (se Figur 30), vilket är en allt vanligare taktik bland cyberkriminella. Attackerna kan automatiseras och skalas upp i en mycket hög takt som vårt experiment visat på och metoder beskrivna av Wahsheh et al. [13].

Jämfört med MDO visade andra säkerhetsverktyg, såsom Eset Premium, Trend Micro QR Scanner och Kaspersky App, en övergripande högre effektivitet i att upptäcka och blockera skadliga QR-koder och phishing-länkar. Speciellt imponerande var Trend Micro QR Scanner, som identifierade samtliga testade skadliga länkar utan några falskt positiva resultat, vilket indikerar en robustare och pålitligare detektionsförmåga.

Den varierande prestandan hos de olika säkerhetsverktygen och särskilt i fallet med MDO understryker behovet av att inte förlita sig enbart på ett enskilt verktyg för att hantera komplexa cyberhot. Istället kan en kombination av flera säkerhetsverktyg, var och en med sina egna styrkor och svagheter, erbjuda ett mer heltäckande skydd för användare mot en mångfald av hot. För användare och organisationer är det därför viktigt att noggrant överväga vilka säkerhetsverktyg som bäst passar deras specifika behov och att komplettera eventuella brister med andra verktyg eller strategier för att säkerställa en hög skyddsnivå.

För att förbättra MDO:s förmåga att hantera skadliga QR-koder och phishing-länkar, särskilt i form av animerade QR-bilder, föreslås ytterligare forskning och utveckling inom området. Det är avgörande att säkerhetsverktyg kontinuerligt uppdateras och förbättras för att möta de ständigt föränderliga hoten på internet och skydda användare mot nya och avancerade former av cyberattacker.

Att uppdatera och implementera extern mjukvara kan vara effektiva åtgärder som kan identifiera och neutralisera hot som annars kan undgå andra säkerhetslösningar. Det kan öka

skyddet signifikant och som nämns i QsecR studien (Rafsanjani et al.) att kontinuerligt informera och uppmuntra anställda till användningen av godkända externa och uppdaterade säkerhetsverktyg. Deras studie betonar också vikten av att tillämpa minsta möjliga privilegier på det systemet som applikationen ska verka i som exempelvis mobiltelefoner. Som säkerhetsansvarig på företaget måste det verifieras att säkerhetsverktyget inte begär och använder andra och känsliga resurser på enheten [14]. Det hade kunnat applicera lösningar såsom QR-kodsskannern från Trend Micro, som uppvisade ett bra resultat utifrån denna studies urval av skadliga Quishing länkar.

För att besvara frågeställningen om: "Hur effektivt är befintliga säkerhetsverktyg, såsom Microsoft Defender for Office, vid upptäckt och blockering av skadliga QR-koder i olika format? " så kan det dras en slutsats kopplat till uppsatsens resultat som tydligt visar på bristande förmåga gentemot andra verktyg som MDO ställdes mot. Detta ger en upplysande bild om att företag som använder MDO som ett verktyg för cybersäkerhet, bör se över fler alternativ när det kommer till verktyg för att hantera svårigheterna när det kommer till detta så pass nya fenomen som är Quishing. Om en organisation vill ha ett heltäckande skydd som företag eller myndighet bör därför användningen av fler verktyg i samordning med MDO ses över.

Det kan även noteras att det företag som uppsatsen skedde i samarbetade med under detta arbete använder MDO som sitt primära verktyg mot hot av denna sort och andra phishing försök. Studien har med dessa resultat klargjort att det inte är ett heltäckande skydd när det kommer till quishing. Studien rekommenderar därför att användning av fler verktyg om företagen vill ha en mer heltäckande lösning mot just quishing.

En koppling kan även göras med dessa resultat för att besvara studiens första frågeställning. Quishing utgör ett växande hot mot företags säkerhet och användares integritet. Resultaten från studiens undersökning ger viktiga insikter om effektiviteten hos olika säkerhetsverktyg för att hantera detta hot, vilket ger en bra grund för att diskutera de potentiella konsekvenserna av den pågående ökningen av quishing.

De konsekvenser som kan uppstå vid fortsatt utveckling av quishing är ökade säkerhetsrisker för både företag men även på individnivå. Utvecklingen bidrar till att phishing attacker i form av quishing kan bli betydligt mycket mer sofistikerade och de blir därav betydligt mycket svårare att upptäcka. Detta kan ses i vårt resultat i koppling med att de verktyg som används för att upptäcka dessa hot direkt fick betydliga svårigheter när det kom till QR koder som inte var statiska.

Ökade säkerhetsrisker för företag:

Resultaten indikerar att säkerhetsverktyg, särskilt Microsoft Defender for Office (MDO) i vissa scenarier, inte är tillräckligt effektiva för att hantera avancerade former av quishing, såsom animerade QR-bilder. Detta innebär att företag som förlitar sig på sådana verktyg kan vara sårbara för attacker och står inför ökade säkerhetsrisker om utvecklingen av quishing fortsätter. Genom att utnyttja brister i säkerhetsverktyg kan angripare infiltrera företagsnätverk, stjäla känslig information och orsaka ekonomiska förluster. Dessutom kan företags anseende och

förtroende skadas om de blir föremål för quishing-attacker, vilket kan få långsiktiga konsekvenser för deras verksamhet och framgång [8].

Hot mot användarnas integritet:

Även om vissa säkerhetsverktyg visar sig vara mer effektiva än andra, blir quishing-attacker alltmer sofistikerade och svåra att upptäcka. Denna utveckling innebär att användare kan bli måltavlor för bedrägeri och identitetsstöld. Genom att locka användare att klicka på skadliga länkar eller lämna ut känslig information kan angripare få tillgång till personliga data såsom lösenord, bankuppgifter och personliga identifieringsuppgifter. Bedragare kan även få åtkomst till företagsdata eller tillgång till företagssystem om en medarbetare blir lurad av en quishing-länk. Personliga data kan sedan även användas för att genomföra bedrägerier, göra obehöriga köp och förstöra användares kreditvärdighet [2]. Dessutom kan identitetsstöld resultera i allvarliga personliga och ekonomiska konsekvenser för drabbade användare, vilket underminerar deras förtroende för digitala tjänster och den övergripande säkerheten på internet.

Sammanfattningsvis så kan det vara relevant att koppla denna information med resultaten från enkäten samt AST:n för att försöka besvara samtliga frågeställningar då även resultaten från experimentet har en påverkan på den tredje frågeställningen, ”Hur kan en organisations säkerhetsåtgärder utformas för att effektivt hantera det växande hotet av quishing med hänsyn till potentiella konsekvenser för företagssäkerhet?” Detta är specifik med MDO:s svaga resultat i åtanke när en plan skapas för företagets hantering och incidentrespons gentemot phishing-hot. Kopplas detta sedan med förslagen från enkäten på hur hanteringen ska gå till i medarbetarnas roll i att minska riskerna för phishing-försök så kan det skapas en relativt heltäckande plan för hur företag ska tänka när det kommer till specifikt phishing-metoder såsom quishing. Denna plan lägger isåfall till på den lista som finns i enkätdiskussionen och skulle se ut såhär:

1. Kontinuerlig utbildning och träning: Eftersom en betydande andel av de anställda saknar relevant IT-utbildning är det viktigt att erbjuda regelbunden utbildning och träning kring olika former av cyberhot, inklusive quishing. Detta kan omfatta att hålla workshops, seminarier och webbinarier där medarbetare får lära sig att känna igen och hantera quishing-attacker.

2. Implementera phishing-simuleringar: Utöver traditionella email phishing-simuleringar bör företaget inkludera former av quishing och vishing i sina simuleringar för att förbereda medarbetare på olika taktiker som används av bedragare. Genom att regelbundet exponera personalen för sådana simuleringar kan de utveckla bättre färdigheter att identifiera och undvika quishing-attacker.

3. Öka medvetenheten om risker: Kommunicera tydligt och regelbundet med de anställda om riskerna med quishing och andra former av cyberhot. Genom att dela exempel, case studies och aktuella händelser relaterade till quishing kan medvetenheten höjas och medarbetarna bli mer engagerade i att aktivt bidra till företagets cybersäkerhet.

4. Skapa en säkerhetskultur: Främja en säkerhetskultur där medarbetarna uppmuntras att vara vaksamma, rapportera misstänkta aktiviteter och ta ansvar för att skydda företagets data och system. Detta kan uppnås genom att belöna goda säkerhetspraxis och integrera säkerhet som en central del av företagets värderingar och arbetskultur.

5. Förbättra tekniskt skydd mot phishing: Överväga att implementera andra verktyg i samverkan med MDO för att få ett mer heltäckande skydd mot nya varianter av phishing såsom quishing eller andra varianter som kan komma att utvecklas i framtiden. Detta för att minska individens roll och den mänskliga faktorn [11] som försvar mot hot genom att filtrera bort skadliga försök redan innan de når medarbetarnas inkorgar.

5. Slutsats

Enkät

Enkätdiskussionen utifrån dess resultat ger tydliga insikter i hur medarbetarna som svarat på studiens enkät har det när det kommer till phishing. Huvudinsikterna som kan extraheras från denna data är en till viss del bristande säkerhetsutbildning när det kommer till cyberhot såsom phishing. Det visar även på att quishing än inte har blivit ett vanligt förekommande fenomen inom de företag där studiens respondenter är medarbetare. Det framkommer dock ändå en tydlig bild av att respondenterna ändå förstår dess allvar och vad som kan bli konsekvenserna om denna form av phishing fortsätter sin drastiska utvecklingskurva som den gjort under de senaste åren. Företag bör därför främja en säkerhetskultur som involverar mer utbildning samt uppmuntran till att vara vaksamma mot phishingförsök och andra relaterade cyberhot genom att visa hur attacker kan gå till och hur en kan ska agera när en individ stöter på phishing. Det är även viktigt att inte bara utbilda i de vanligaste formerna av phishing, som vi ser indikationer på i enkäten, utan även att utbilda och visa hur andra former av phishing kan visa sig och hur dessa kan hanteras.

AST

Sammanfattningsvis visar resultaten en positiv utveckling i medarbetarnas förmåga att hantera phishinghot, men understryker också behovet av fortsatta anpassningar och variationer i framtida säkerhetsträningar. Ökningen i rapporteringen från januari till mars och en minskning i april tyder på att olika typer av simuleringar påverkar deltagarnas beteenden olika, vilket understryker vikten av att kontinuerligt anpassa säkerhetsinterventionerna efter rådande säkerhetsmiljö och specifika arbetsplatskulturer. För att effektivt hantera hotet från quishing, bör Microsoft och andra aktörer överväga att implementera omfattande och proaktiva säkerhetsutbildningar som specifikt adresserar riskerna med QR-koder. Detta bör inkludera utvecklingen av läromoduler som är speciellt utformade för att utbilda anställda om riskerna med modifierade eller bedrägliga QR-koder, både i e-post och i fysiska miljöer. Genom att stärka dessa utbildningsprogram kan företag inte bara förbättra den individuella medarbetarens förmåga att identifiera och undvika quishing-attacker, utan också förbättra den övergripande cybersäkerhetsposturen i en alltmer digitaliserad fordonsindustri.

Experiment

När sammanfattningen av experimentet är färdigställt så har arbetet kommit fram till en slutsats som innebär att det finns en tydlig brist i MDO:s förmåga att detektera olika former av quishing i jämförelse med andra verktyg som blev tilldelade samma uppgift. Resultaten var tydliga och en uträkning av error-bars med ett kofidensintervall på 95% gjordes för att stärka denna bild och med dessa så blir resultatet ännu säkrare på att MDO för tillfället ligger efter när det kommer till just denna form av phishing.

Studien rekommenderar alltså fler företag att fortsätta med kontinuerlig utbildning och testning av personal för att säkerställa att de är så vaksamma och underrättade som möjligt. För att utveckla denna utbildning så rekommenderas även att implementera testning och utbildning av personal på andra metoder såsom quishing för att minska risken för att dessa nya former av

attacker kan komma att äventyra företagets eller individens integritet. Detta ser författarna helst att det implementeras så snabbt som möjligt. Detta trots att studiens undersökning indikerar på att quishing än inte blivit ett vanligt förekommande fenomen bland studiens respondenter. Men för att försöka ligga steget före så rekommenderar studien då att börja med det så snabbt som möjligt.

All denna information har bidragit med en tydlig bild över vad som behöver förbättras både tekniskt och kunskapsmässigt när det kommer till företagets medarbetare. Det har alltså bidragit med tydliga svar på arbetets frågeställningar:

1. Vilka strategier och metoder är mest effektiva för att höja medarbetares medvetenhet och engagemang i att förebygga quishing och andra relaterade cyberhot?

2. Hur effektivt är befintliga säkerhetsverktyg, såsom Microsoft Defender for Office, vid upptäckt och blockering av skadliga QR-koder i olika format?

3. Hur kan en organisations säkerhetsåtgärder utformas för att effektivt hantera det växande hotet av quishing med hänsyn till potentiella konsekvenser för företagssäkerhet?

Dessa frågeställningar kan sammanfattningsvis snabbt besvaras i punktform på följande vis som gjorts i diskussionen. Det kan även komma att fungera som en allmän rekommendation till företag att försöka implementera stegen från denna lista för att få en bättre hantering och incidentrespons när det kommer till phishing och andra cyberhot av liknande natur:

1. Kontinuerlig utbildning och träning: Eftersom en betydande andel av de anställda saknar relevant IT-utbildning är det viktigt att erbjuda regelbunden utbildning och träning kring olika former av cyberhot, inklusive quishing. Detta kan omfatta att hålla workshops, seminarier och webbinarier där medarbetare får lära sig att känna igen och hantera quishing-attacker.

2. Implementera phishing-simuleringar: Utöver traditionella email phishing-simuleringar bör företaget inkludera former av quishing och vishing i sina simuleringar för att förbereda medarbetare på olika taktiker som används av bedragare. Genom att regelbundet exponera personalen för sådana simuleringar kan de utveckla bättre färdigheter att identifiera och undvika quishing-attacker.

3. Öka medvetenheten om risker: Kommunicera tydligt och regelbundet med de anställda om riskerna med quishing och andra former av cyberhot. Genom att dela exempel, case studies och aktuella händelser relaterade till quishing kan medvetenheten höjas och medarbetarna bli mer engagerade i att aktivt bidra till företagets cybersäkerhet.

4. Skapa en säkerhetskultur: Främja en säkerhetskultur där medarbetarna uppmuntras att vara vaksamma, rapportera misstänkta aktiviteter och ta ansvar för att skydda företagets data och system. Detta kan uppnås genom att belöna goda säkerhetspraxis och integrera säkerhet som en central del av företagets värderingar och arbetskultur.

5. Förbättra tekniskt skydd mot phishing: Överväga att implementera andra verktyg i samverkan med MDO för att få ett mer heltäckande skydd mot nya varianter av phishing såsom quishing eller andra varianter som kan komma att utvecklas i framtiden. Detta för att minska individens roll och den mänskliga faktorn som försvar mot hot genom att filtrera bort skadliga försök redan innan de når medarbetarnas inkorgar.

5.1 Framtida forskning

Denna studie fungerar som ett viktigt och bra startskott för framtida forskning inom området quishing och dess risker. Genom att utforska och identifiera potentiella trender och systematiska förändringar inom företagens cybersäkerhet har det skapats en grundläggande förståelse som andra forskare kan studera vidare. Det är viktigt att betona att resultaten från analyserna, inklusive de från AST och det experimentella testet, endast indikerar möjliga samband och inte etablerar definitiva orsakssamband. Medan det användes medelvärden för att illustrera resultaten, bör dessa uppfattas som skattningar av det förväntade förhållandet snarare än exakta värden, vilket understryker betydelsen av att ta hänsyn till slumpmässigheten i datainsamlingen och de inneboende varianserna med individuella svar. Detta arbete lägger en viktig grund för framtida studier, där andra forskare kan utforska dessa resultat djupare och verifiera studiens resultat.

Då MDO inte var lika effektivt mot animerade QR-koder skulle det, i framtida forskningar kunna utforskas ytterligare genom fler empiriska tester, detta för att bättre förstå verktygets begränsningar.

5.2 Rekommendationer för förbättrad säkerhetsutbildning

Resultaten som framkom tyder på att det finns ett behov av att utvidga omfånget av säkerhetsutbildningar för att inkludera inte bara traditionella hot som e-post och länkar, utan även nyare och mer aktuella former av hot. Denna anpassning av utbildningsinnehållet bör syfta till att öka de anställdas medvetenhet och beredskap inför nya angreppsmetoder.

Integreringen av Zero Trust-principer erbjuder ett robust sätt att minska effekten av quishing-attacker. Genom att säkerställa att varje försök till åtkomst noggrant kontrolleras och begränsas kan organisationer effektivt minska sin attackyta och förbättra sin övergripande cybersäkerhet. Denna strategi, tillsammans med en ökad medvetenhet och utbildning kring cyberhot, är avgörande för att skydda både organisatoriska och personliga data. Samtidigt understryker resultaten vikten av både ett individuellt och organisatoriskt ansvar för att bekämpa spridningen av skadligt material. Individer bör uppmuntras att aktivt delta i säkerhetsutbildningar och tillämpa säkerhetspraxis i sin dagliga verksamhet. För arbetsgivare pekar studien på nödvändigheten av att implementera säkerhetsarkitekturer baserade på principerna om zero trust och least privilege. Dessa strategier är avsedda att minimera risken och begränsa skadeverkningarna av mänskliga misstag, vilket är den svagaste länken i skyddet mot phishing. Men att prata mer om detta ämne efterfrågas av många av respondenterna i studiens enkätundersökning och nu har denna studie ökat medvetenheten ett snäpp högre ute bland företagen.

Referenser

[1] F. Sharevski, A. Devine, E. Pieroni, och P. Jachim, ”Phishing with Malicious QR Codes”, i *Proceedings of the 2022 European Symposium on Usable Security*, Karlsruhe Germany: ACM, sep. 2022, s. 160–171. doi: 10.1145/3549015.3554172.

[2] R. Hoheisel, G. van Capelleveen, D. K. Sarmah, och M. Junger, ”The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains”, *Comput. Secur.*, vol. 128, s. 103158, maj 2023, doi: 10.1016/j.cose.2023.103158.

[3] Society for Human Resource Management, ”QR Code Phishing Attacks Spread: Employees must be trained to recognize a growing threat”, *HRNews*, aug. 2023, Åtkomstdatum: 31 januari 2024. [Online]. Tillgänglig vid: https://www.proquest.com/docview/2858314405/citation/CC60FD081B0A4A2FPQ/1

[4] P. Muncaster, ”Police Issue “Quishing” Email Warning”, Infosecurity Magazine. Åtkomstdatum: 03 februari 2024. [Online]. Tillgänglig vid: https://www.infosecurity-magazine.com/news/police-issue-quishing-email-warning/

[5] ”Zscaler ThreatLabz Research Shows a Nearly 50% Increase in Phishing Attacks with Education, Finance, and Government Being the Most Targeted: Annual Phishing Report Highlights New and Evolving Phishing Campaigns Resulting from the Rise of AI Platforms, like ChatGPT, Urges Organizations to Adopt a Zero Trust Architecture”, *NASDAQ OMX's News Release Distribution Channel*, NASDAQ OMX Corporate Solutions, Inc., New York, United States, 18 april 2023. Åtkomstdatum: 03 maj 2024. [Online]. Tillgänglig vid: https://www.proquest.com/docview/2802214250/citation/A030187E3A194894PQ/1

[6] M. Chapple, J. M. Stewart, och D. Gibson, *(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide*. Newark, UNITED STATES: John Wiley & Sons, Incorporated, 2021. Åtkomstdatum: 03 maj 2024. [Online]. Tillgänglig vid: http://ebookcentral.proquest.com/lib/halmstad/detail.action?docID=6647278

[7] A. A. Jillepalli,et Al., ”Enterprise-level Hardening of Web Browsers for Microsoft Windows”, *Int. J. Comput. Digit. Syst.*, vol. 7, nr 5, s. 261–274, sep. 2018, doi: 10.12785/ijcds/070501.

[8] E. E. H. Lastdrager, ”From fishing to phishing”, feb. 2018, doi: 10.3990/1.9789036544795.

[9] gmcdouga, ”Conditional QR Code Routing Attacks”, Check Point Blog. Åtkomstdatum: 01 februari 2024. [Online]. Tillgänglig vid: https://blog.checkpoint.com/harmony-email/conditional-qr-code-routing-attacks/

[10] J. Rodriguez, ”-Stories from the SOC: Quishing – Combatting embedded malicious QR codes”. Åtkomstdatum: 01 februari 2024. [Online]. Tillgänglig vid: https://cybersecurity.att.com/blogs/security-essentials/stories-from-the-soc-quishing-combatting-embedded-malicious-qr-codes

[11] M. för samhällsskydd och beredskap MSB, ”Cyberangrepp mot samhällsviktiga informationssystem : 25 rekommendationer för stärkt skydd mot cyberangrepp”. Åtkomstdatum: 03 februari 2024. [Online]. Tillgänglig vid: https://www.msb.se/sv/publikationer/cyberangrepp-mot-samhallsviktiga-informationssystem--25-rekommendationer-for-starkt-skydd-mot-cyberangrepp/

[12] T. Vidas, E. Owusu, S. Wang, C. Zeng, L. Cranor, och N. Christin, ”QRishing : The Susceptibility of Smartphone Users to QR Code Phishing Attacks”, *Springer*, vol. 7862, 52-69,2013, 2013, [Online]. Tillgänglig vid: https://kilthub.cmu.edu/ndownloader/files/11896547

[13] H. A. M. Wahsheh och M. S. Al-Zahrani, ”Secure Real-Time Computational Intelligence System Against Malicious QR Code Links”, *Int. J. Comput. Commun. CONTROL*, vol. 16, nr 3, Art. nr 3, maj 2021, Åtkomstdatum: 07 februari 2024. [Online]. Tillgänglig vid: https://univagora.ro/jour/index.php/ijccc/article/view/4186

[14] A. S. Rafsanjani, N. B. Kamaruddin, H. M. Rusli, och M. Dabbagh, ”QsecR: Secure QR code Scanner According to a Novel Malicious URL Detection Framework”, *IEEE Access*, vol. 11, s. 1–1, 2023, doi: 10.1109/ACCESS.2023.3291811.

[15] N. Beu *m.fl.*, ”Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation”, *Comput. Secur.*, vol. 131, s. 103313, aug. 2023, doi: 10.1016/j.cose.2023.103313.

[16] D. Timko och M. L. Rahman, ”Commercial Anti-Smishing Tools and Their Comparative Effectiveness Against Modern Threats”. arXiv, 14 september 2023. Åtkomstdatum: 04 mars 2024. [Online]. Tillgänglig vid: http://arxiv.org/abs/2309.07447

[17] A. El Aassal och R. Verma, ”Spears Against Shields: Are Defenders Winning the Phishing War?”, i *Proceedings of the ACM International Workshop on Security and Privacy Analytics*, Richardson Texas USA: ACM, mar. 2019, s. 15–24. doi: 10.1145/3309182.3309191.

[18] ”Microsoft Defender for Office 365 | Microsoft Security”. Åtkomstdatum: 07 februari 2024. [Online]. Tillgänglig vid: https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365

[19] Microsoft Learn, ”Get started using Attack simulation training”. Åtkomstdatum: 07 februari 2024. [Online]. Tillgänglig vid: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide

[20] ”Train your users to be more resilient against QR code phishing”, TECHCOMMUNITY.MICROSOFT.COM. Åtkomstdatum: 01 maj 2024. [Online]. Tillgänglig vid: https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/train-your-users-to-be-more-resilient-against-qr-code-phishing/ba-p/4022667

[21] A. Bryman, *Samhällsvetenskapliga metoder*, Upplaga 3. Stockholm: Liber, 2018.

[22] D. Åkerlund, *Guide till akademiskt skrivande om att skriva rapporter, uppsatser och självständiga skriftliga arbeten på universitet och högskolor*. Karlstad: s universitet, 2016.

[23] ”Fortune Global 500 – The largest companies in the world by revenue”, Fortune. Åtkomstdatum: 01 april 2024. [Online]. Tillgänglig vid: https://fortune.com/ranking/global500/2023/search/

[24] ”19 Most Common Types of Phishing Attacks in 2024 | UpGuard”. Åtkomstdatum: 03 maj 2024. [Online]. Tillgänglig vid: https://www.upguard.com/blog/types-of-phishing-attacks

[25] ”The Latest Phishing Statistics (updated April 2024) | AAG IT Support”. Åtkomstdatum: 03 maj 2024. [Online]. Tillgänglig vid: https://aag-it.com/the-latest-phishing-statistics/

Appendix

Appendix A

Formulär: https://forms.office.com/e/WspMrK08iT

Fig. 32. Enkätens framsida med vilken information respondenterna fick innan de tog del av enkäten.

Frågorna som kommer att ställas i enkätundersökningen finner ni här

1.

Fig. 33. Fråga 1 enkät.

2.

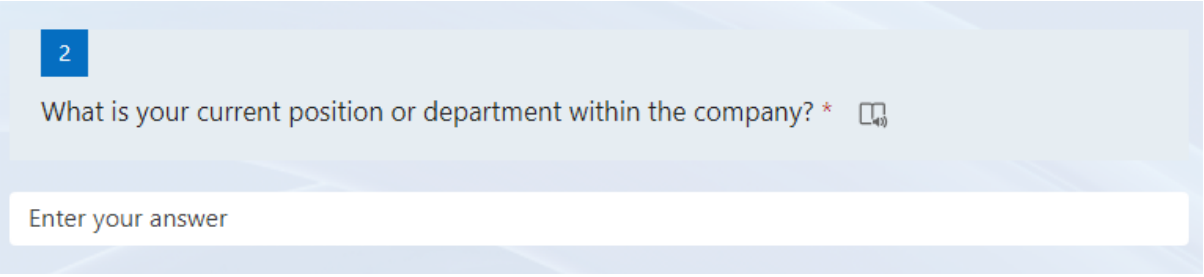

Fig. 34. Fråga 2 enkät

3.

Fig. 35. Fråga 3 enkät

4.

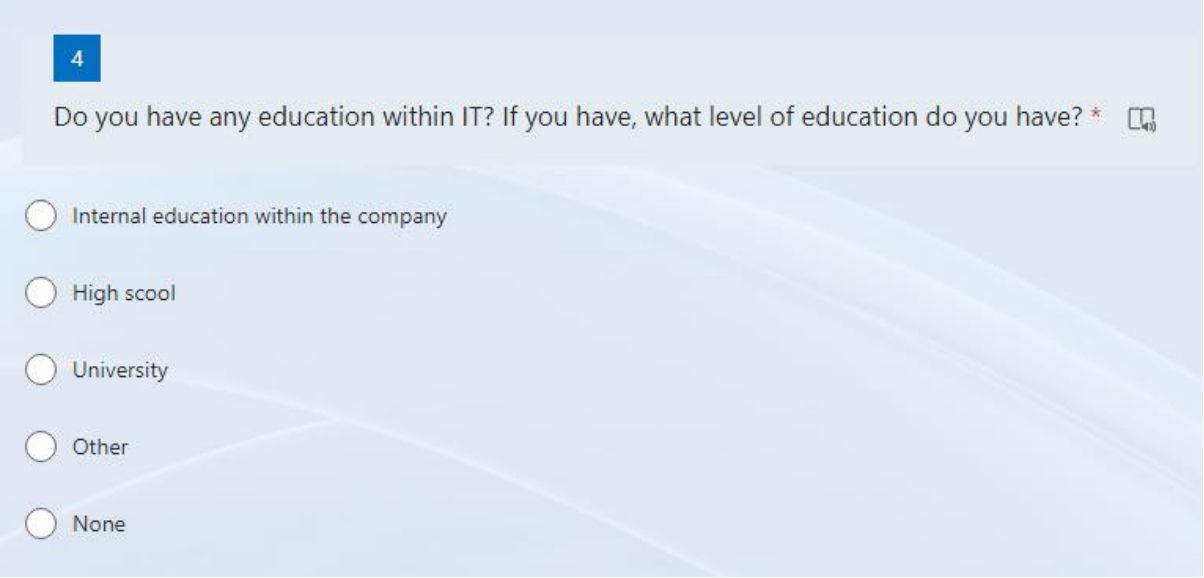

Fig. 36. Fråga 4 enkät

5.

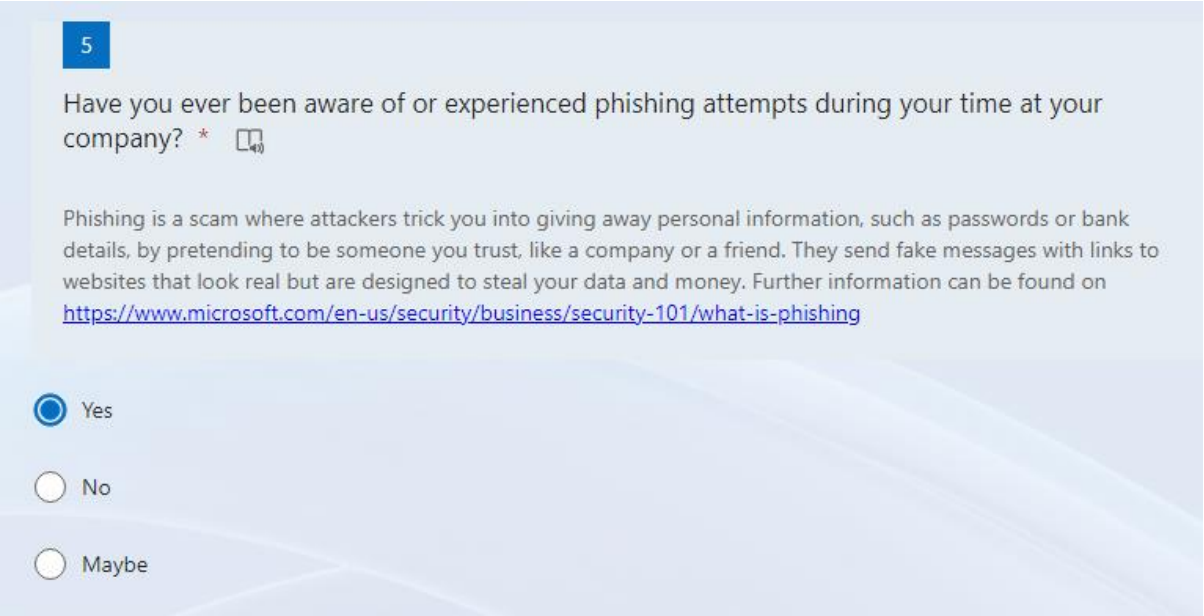

Fig. 37. Fråga 5 enkät

6.

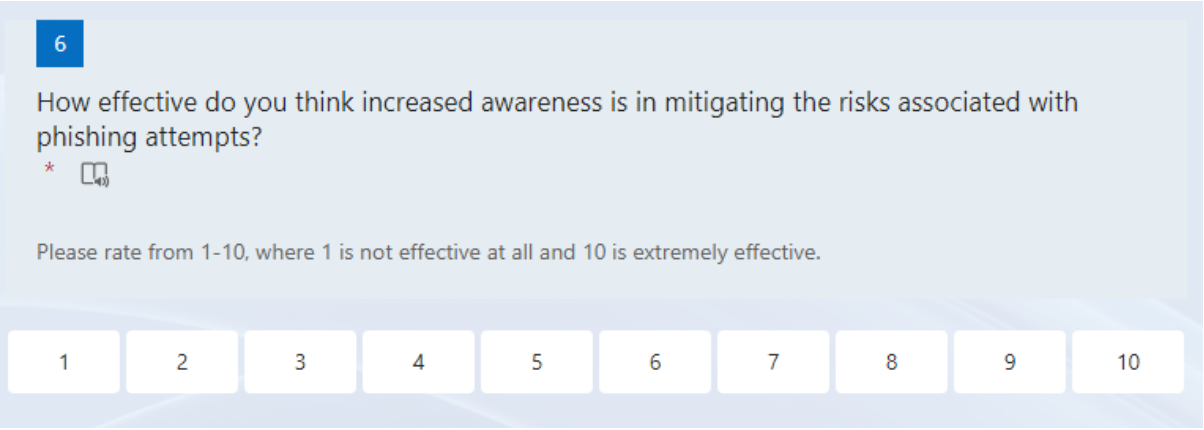

Fig. 38. Fråga 6 enkät

7.

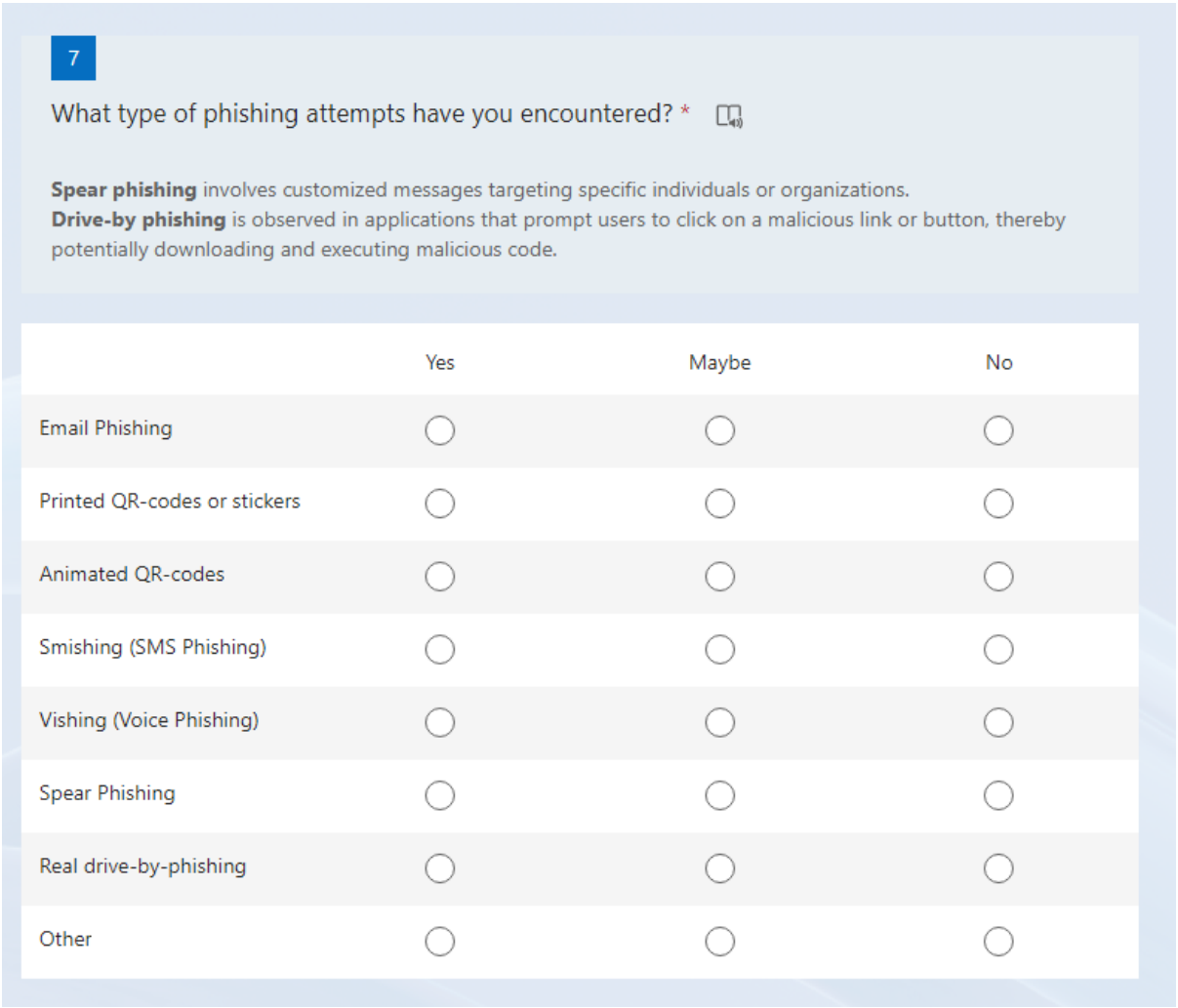

Fig. 39. Fråga 7 enkät

8.

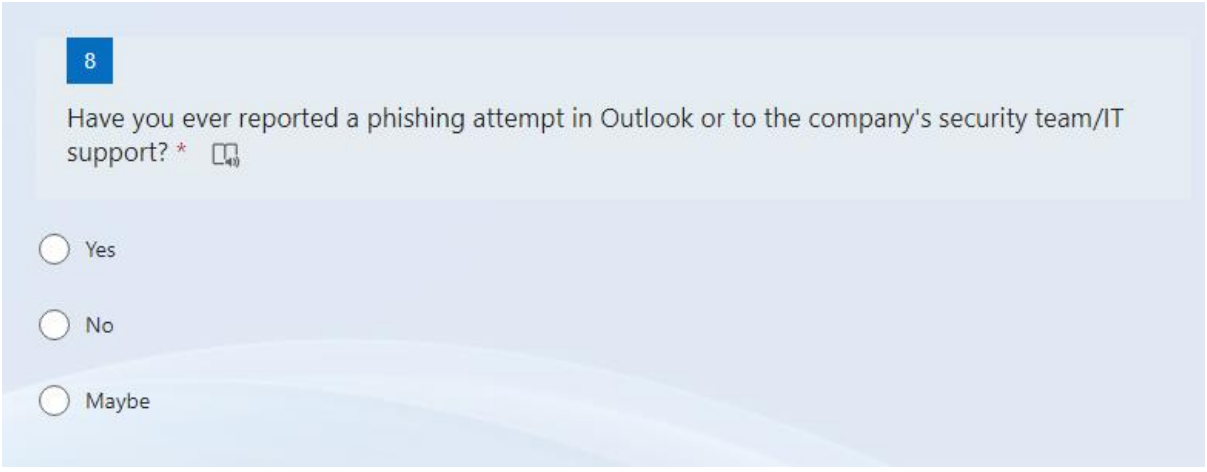

Fig. 40. Fråga 8 enkät

9.

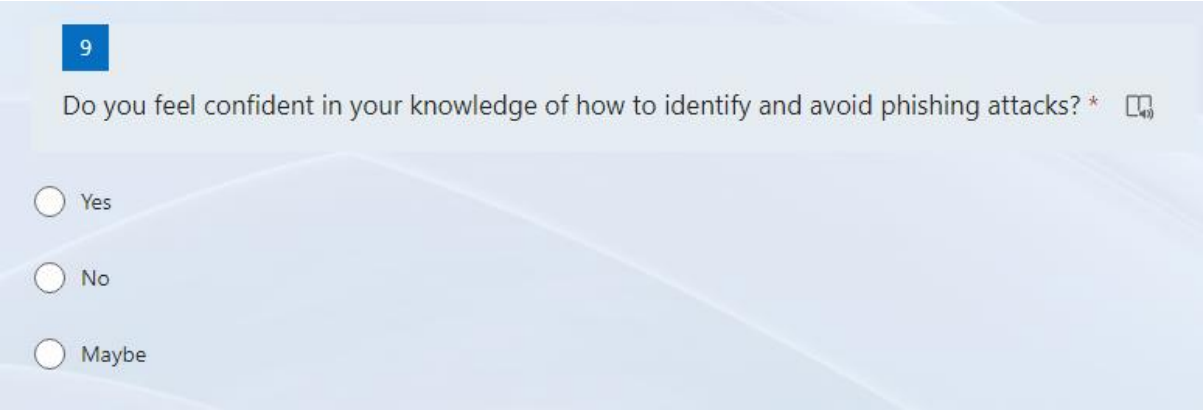

Fig. 41. Fråga 9 enkät

10.

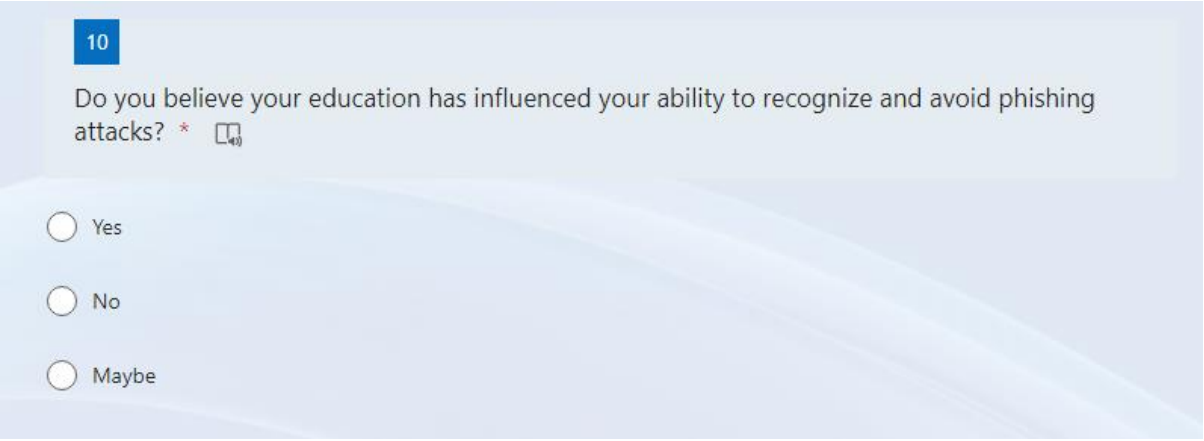

Fig. 42. Fråga 10 enkät

11.

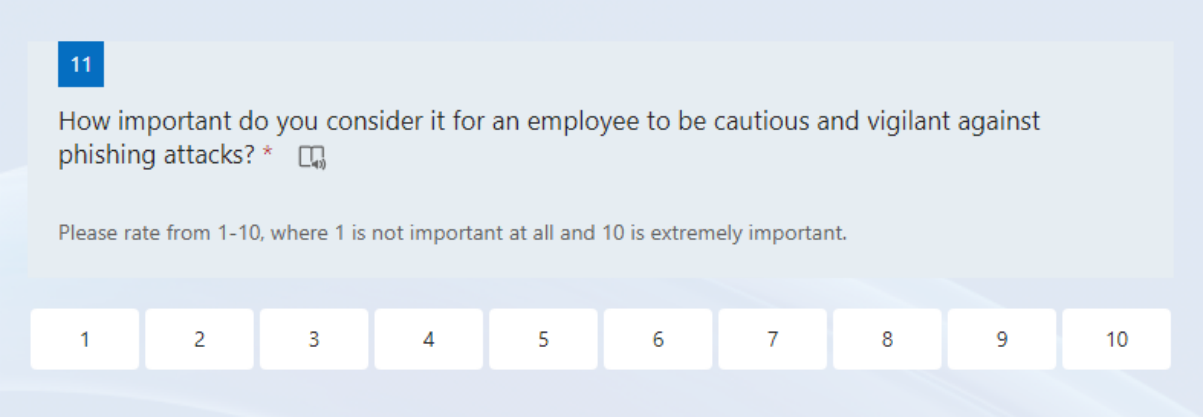

Fig. 43. Fråga 11 enkät

12.

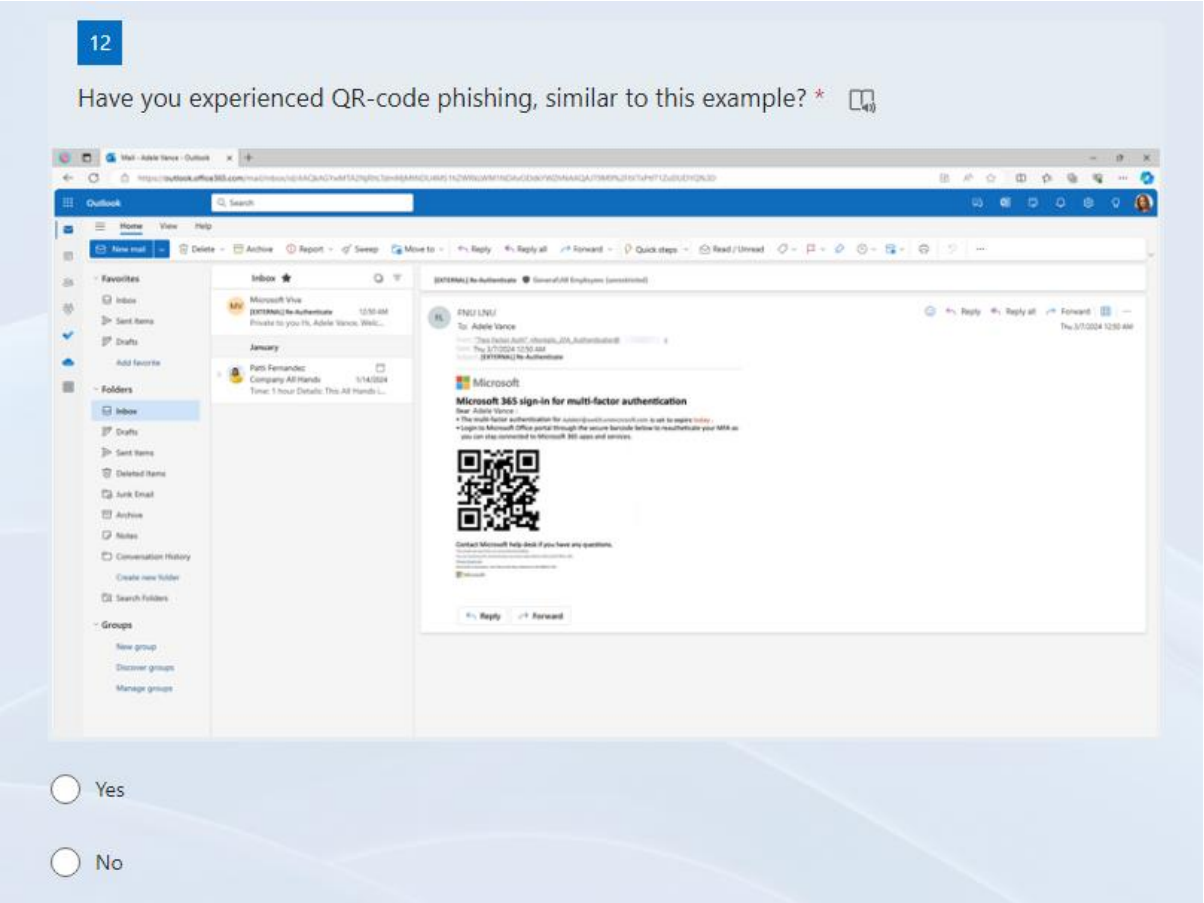

Fig. 44. Fråga 12 enkät

13.

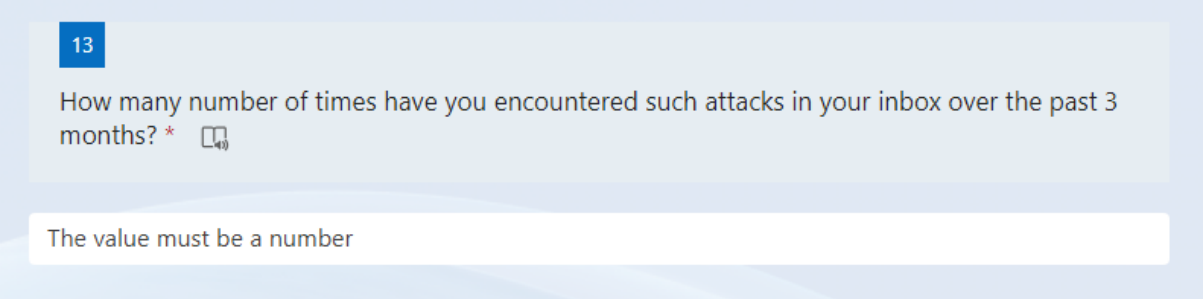

Fig. 45. Fråga 13 enkät

14.

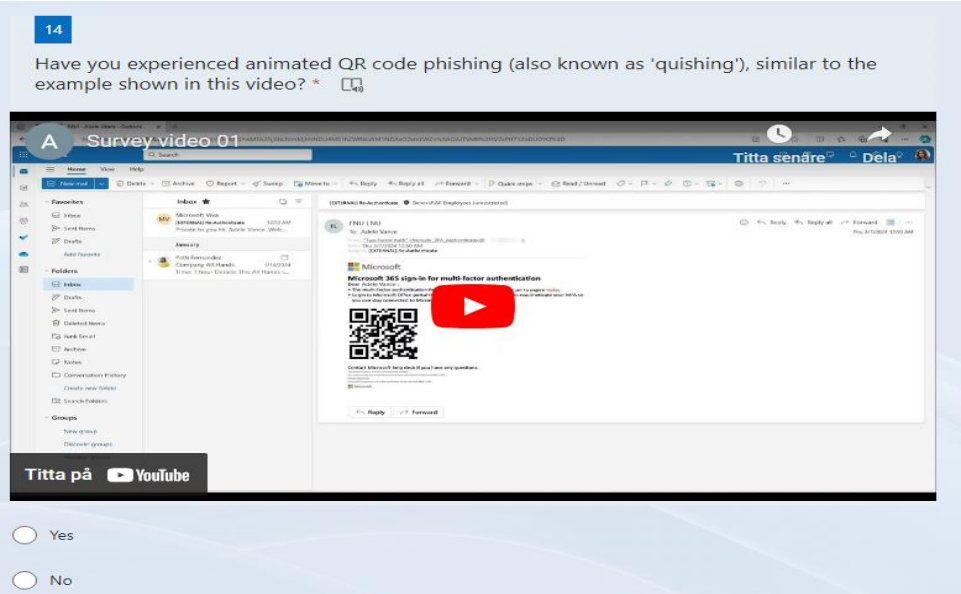

Fig. 46. Fråga 14 enkät

Länk till video:
https://www.youtube.com/watch?time_continue=1&v=1E7HDskAIHA&embeds_referring_euri=https%3A%2F%2Fforms.office.com%2F&source_ve_path=MjM4NTE&feature=emb_title

15.

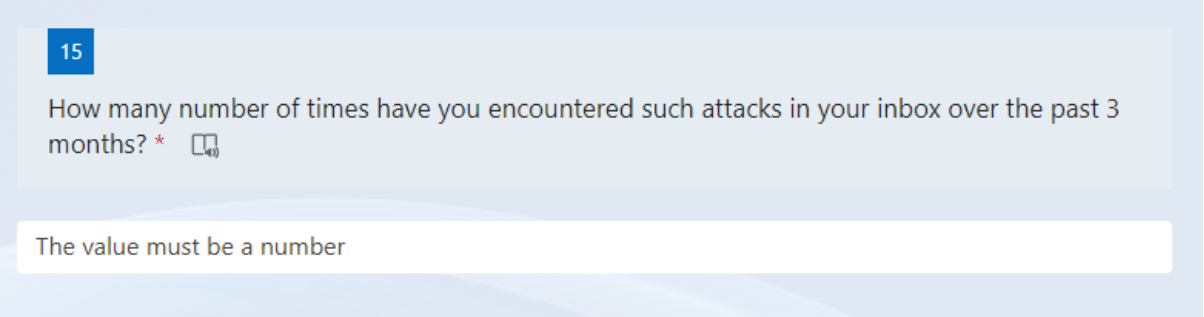

Fig. 47. Fråga 15 enkät

16.

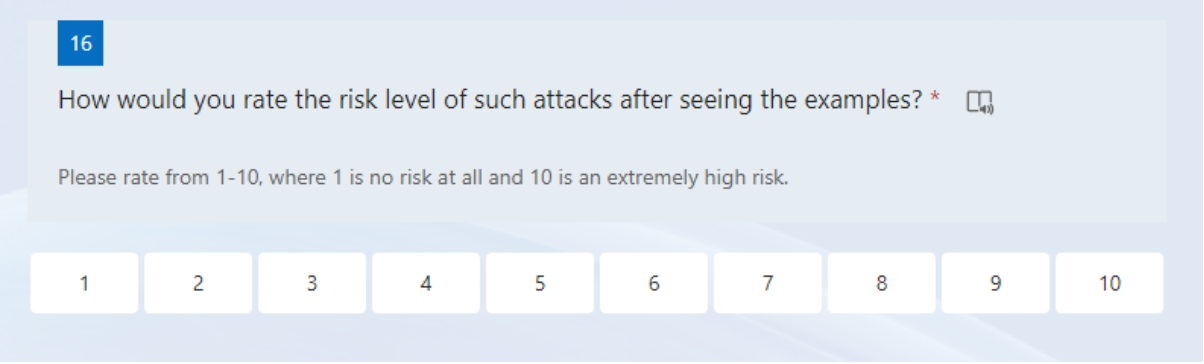

Fig. 48. Fråga 16 enkät

17.

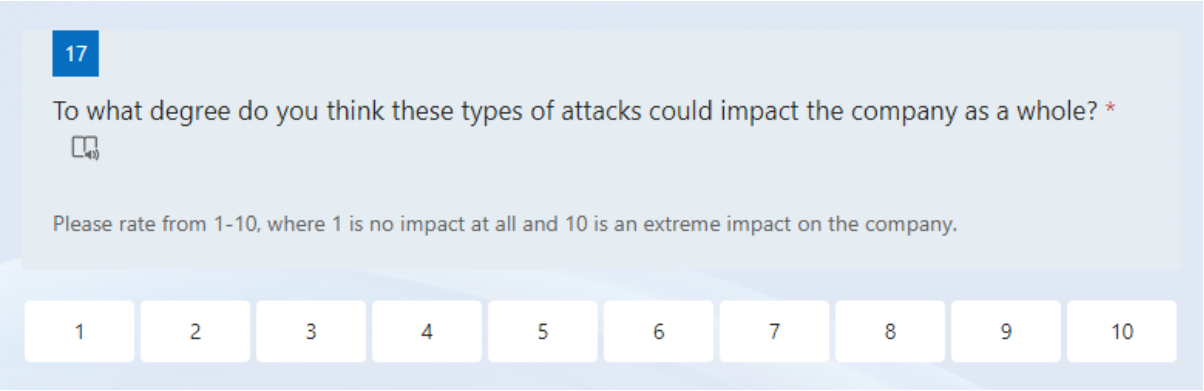

Fig. 49. Fråga 17 i enkäten, respondenten uppmanas att betygsätta på en skala till vilken grad de tror att attacken kan påverka deras arbetsplats.

18.

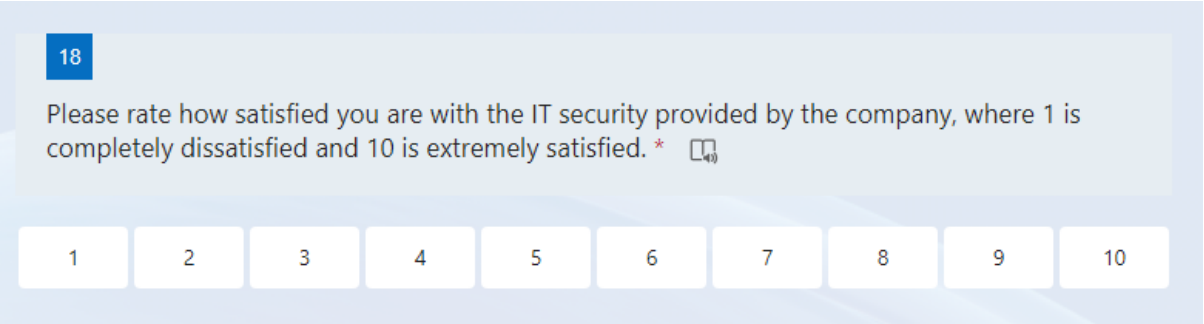

Fig. 50. Fråga 18 enkät

19.

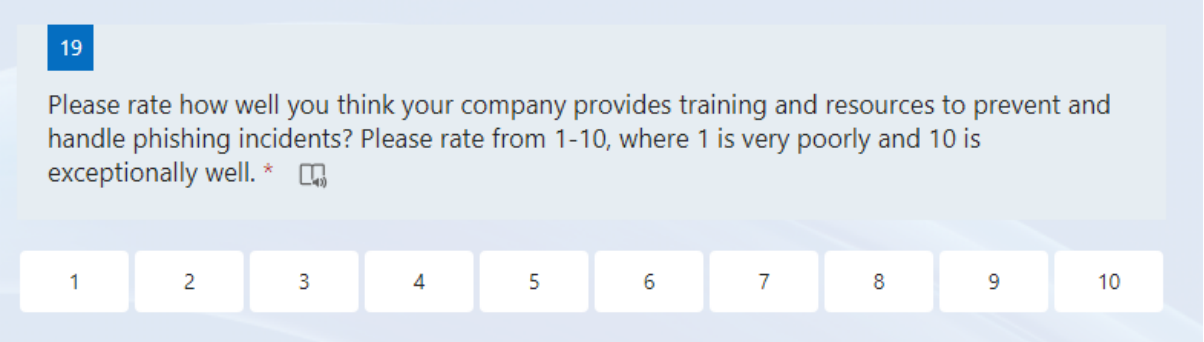

Fig. 51. Fråga 19 enkät

20.

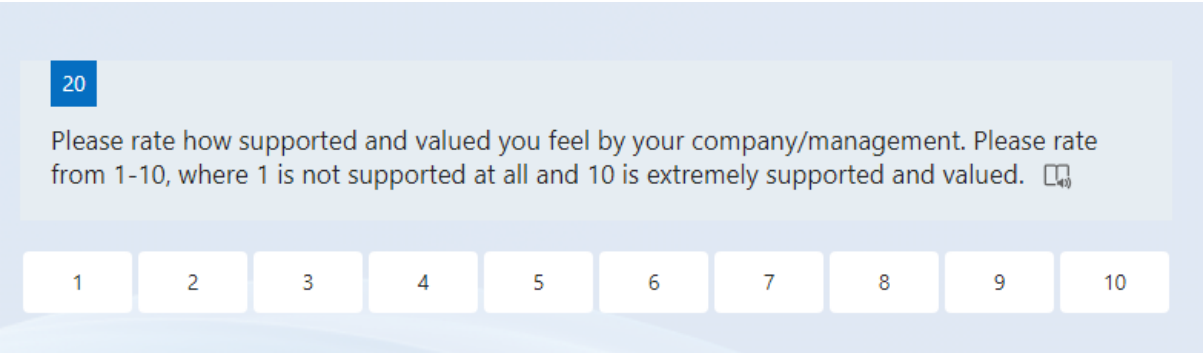

Fig. 52. Fråga 20 enkät

21.

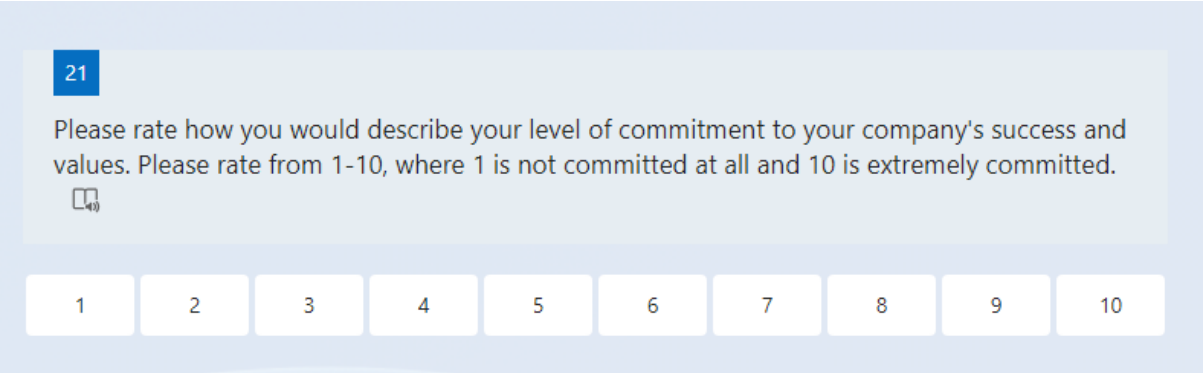

Fig. 53. Fråga 21 enkät

22.

Fig. 54. Fråga 22 enkät

23.

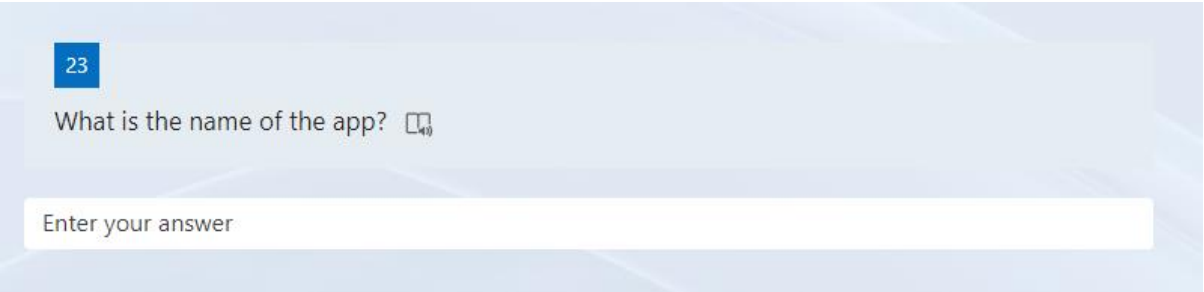

Fig. 55. Fråga 23 enkät

24.

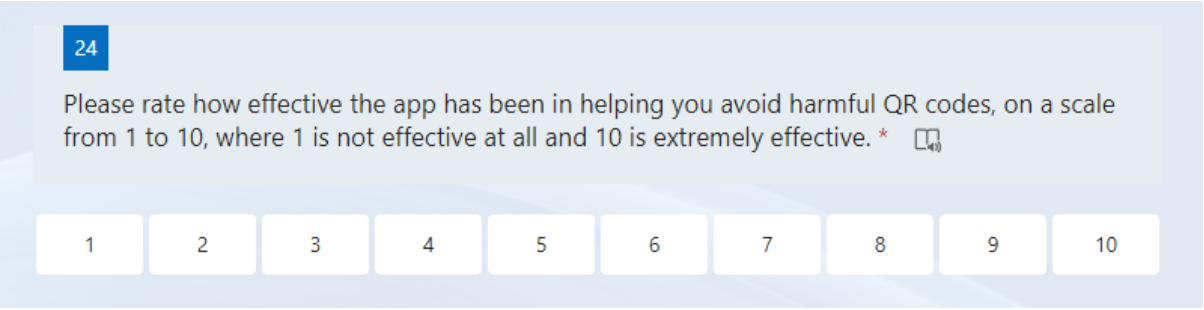

Fig. 56. Fråga 24 enkät

25.

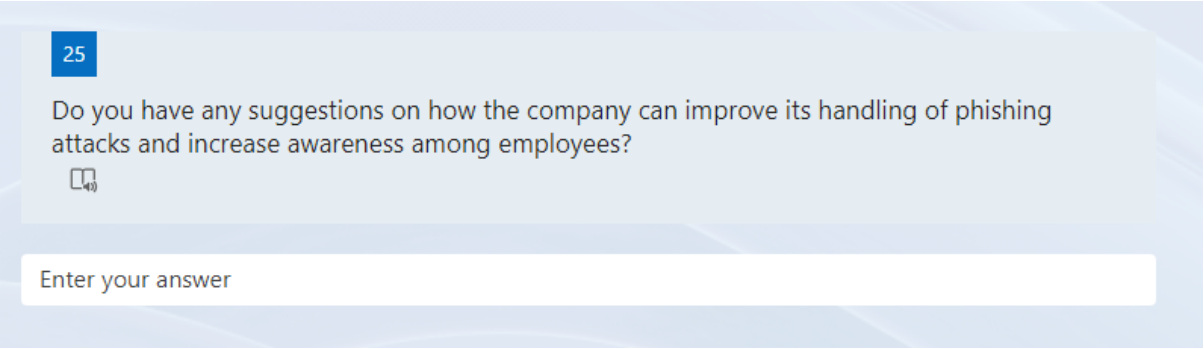

Fig. 57. Fråga 25 enkät

Appendix B

Svar på fråga 2 i enkäten, komplett lista som även inkluderar svar som siffror eller frågetecken:

1 Ekonomi-assistent
2 Säljare
3 Assistent
4 Soc analytiker
5 VD
6 Chef
7 Tillsvidareanställd
8 HR
9 Ekonomi
10 IT
11 Projektchef
12 Nättekniker
13 CFO
14 Ekonomiassistent
15 Kassaledare
16 Studentmedarbetare
17 Studentmedarbetare
18 Unified Production & Logistics worker
19 Software Developer
20 IT
21 Väktare
22 Säkerhetsanalytiker
23 Incidenten och Problemmanager
24 Enhetschef
25 Sekreterare
26 Administratör
27 ?
28 Snickare
29 Anställd
30 Vd
31 ScrumMaster
32 0
33 Projektledare
34 Läkare
35 Administratör
36 Tekniker
37 Studerande
38 Lagerarbetare

39 2
40 Kurator
41 AT-läkare
42 Account manager
43 Mekaniker
44 Redaktör
45 Lagerarbetare
46 Projektledare elkraft
47 Undersköterska
48 Första linjens chef
49 Anställd
50 Bäst
51 Undersköterska
52 Anställd
53 Operatör
54 Consultant
55 Administration och patient behandling.
56 Universitetsadjunkt
57 Undersköterskan
58 Chaufför
59 Marketing
60 Worker
61 Varumottagning
62 Kök
63 Medarbetare
64 Cyber Security Consultant
65 Manufacturing Engineering
66 Specialist
67 Customer Care
68 IT Cybersecurity Expert
69 Business Transformation & Retailer Development
70 R&Dengineering
71 Developer
72 Homologation
73 Union representative
74 Adjunkt lärarutbildningen
75 Data Architect in Digital Core
76 Leading function in Supply Chain
77 HR Manager
78 Design leader
79 Test engineer
80 Senior Site-SPM Engineer
81 Secure Identity Techlead

82 CISO
83 Biomedicinsk analytiker

Komplett lista med svar från fråga 25 i enkäten som även inkluderar svar som anses vara icke-kompletta eller orelevanta:

1. Utbilda personal

2. Man kan berätta för personerna inom företaget att man ska vara försiktig med länkar osv.

3. Utbildning

4. Ja, fortsatta tydliga policyer och utbildningar för personalen oavsett vilken avdelning de sitter på.

5. Nej

6. Ja det gäller väl att främja en företagskultur som ständigt jobbar med att öka de anställdas medvetenhet om hot som dessa.

7. Vet inte, mitt företag är ganska bra på att hantera och motverka phishing

8. Nej

9. Utbilda i samtliga typer av phishing-attacker, det är stort fokus på phishing via mejl

10. Education

11. Nej

12. ?

13. Limiterad användning av Mail samt telefon.

14. Skicka ännu fler mail antar jag.

15. My company already filters all emails sent to the company email, since i have not recieved or noticed any phising attempts at all, i would assume that the current methods are working very well, and can therefore not think of anything they could improve.

16. Nej

17. Nej

18. Utbildning

19. Genom återkommande utbildningar och även fejkade phising mail

20. He

21. Agera proaktivt, informera om riskerna och skapa medvetenhet genom att visa exempel på hur en attack kan gå till.

22. Nej

23. Nej det fungerar fint, de har bra koll och kontinuerliga ”tester” på alla oss anställda

24. Ingen aning

25. Nej

26. Nej

27. Jag är inte anställd någonstans.

28. Utbilda

29. Regelbunden utbildning av personalen. På min arbetsplats får vi ca varannan vecka frågor kring It-säkerhet som vi besvarar. Tar ca 5 min att fylla i. Därutöver testas vi regelbundet genom att falska mejl med länkar skickas.

30. Vet ej tyvärr

31. -

32. Ha koll på medarbetare internet användning

33. Sätta upp en sån nice lapp i fikarummet "klicka inte på några länkar"

34. Nej inte direkt. Kanske prata mer om det och inte bara via email-utbildningar.

35. Vet ej

36. Kontinuerlig utbildning

37. Anställa kompetent IT-personal med rätt förutsättningar för att motverka eller identifiera potentiella attacker.

38. Dom ska ge fan i att trycka på kattvideor och miljonvinster från Afrika! Sen kan de ge fan i att öppna filer på mailen som Outlook varnar om bestämt som .Exe filer.

39. Nej ev mera utbildning

40. Nej, fortsätter att arbetas kontinuerligt med detta. Både genom fejk meddelande och utbildning. Hellre ta bort ett mejl för mycket och få en påminnelse.

41. Genom kontinuerlig intern utbildning

42. Mer utbildning

43. Det är en bra fråga. Vi går igenom en hel del kurser för att känna igen inkräktare på våra mail och via fake sidor. Qr koder har vi inte gått igenom så mycket

44. No

45. Mer kontakt och bättre hantering. Större empati och förståelse

46. Yes, more training excercises and meetings for all kinds of Phishing attacks with a focus on specifically the QR Code, Animated QR Code and Voice Phishing attacks.

47. Short training are really good, keep it doing.

48. No

49. Continue with reminders and training

50. Run more simulations, spear-phishing specifically. Implement features in the employees inbox applications that makes it extremely clear what to look out for at all times. Give employees access to virtual environments to test links before actually using them. 1984-mode: Restrict access to html emails and that will be the end of it.

Appendix C

Python script som skapar en loading gif-animation med en inbäddad QR-kod, med möjligheten att importera e-postadresser från addresses.csv och URL.

```
import imageio
from PIL import Image, ImageDraw, ImageFont
import math
import qrcode
from urllib.parse import quote, urlparse
import base64
import csv
import os

# Create loading GIF
def create_loading_gif(filename, resolution=(600, 600), duration=3):
    images = []
    num_frames = 100  # Frame count

    for i in range(num_frames):
        img = Image.new('RGB', resolution, color='white')
        draw = ImageDraw.Draw(img)

        # Font for loading text
        font = ImageFont.truetype("segoeui.ttf", 40)

        # Draw loading text
        text = 'Loading...'
        text_width, text_height = draw.textsize(text, font=font)
        text_position = ((resolution[0] - text_width) // 2, (resolution[1] - text_height) // 2)
        draw.text(text_position, text, fill='black', font=font)

        # Draw dots around loading text
        num_dots = 12  # Number of dots
        for j in range(num_dots):
            angle = (i + j * (360 / num_dots)) * (360 / num_frames)
            radius = 100  # Increase radius
            dot_x = resolution[0] // 2 + int(radius * 1.2 * math.cos(math.radians(angle)))
            dot_y = resolution[1] // 2 + int(radius * 1.2 * math.sin(math.radians(angle)))
```

```
            draw.ellipse((dot_x - 8, dot_y - 8, dot_x + 8, dot_y + 8), fill='black')  # Increased the dot size
        images.append(img)
    imageio.mimsave(filename, images, duration=duration)
# Create a static QR code
def create_static_qr_gif(text, filename, resolution=(600, 600), duration=60):
    images = []
    num_frames = 1500

    for i in range(num_frames):
        img = Image.new('RGB', resolution, color='white')
        draw = ImageDraw.Draw(img)

        # Draw QR code without URL encoding
        qr = qrcode.QRCode(version=1, box_size=20, border=10)
        qr.add_data(text)  # Use the original text without URL encoding
        qr.make(fit=True)
        qr_img = qr.make_image(fill_color="black", back_color="white")
        qr_img = qr_img.resize(resolution, Image.ANTIALIAS)
        img.paste(qr_img, (0, 0))

        images.append(img)

    imageio.mimsave(filename, images, duration=duration)  # Duration is in seconds

# Get domain name from URL
def get_domain_name(url):
    parsed_url = urlparse(url)
    return parsed_url.netloc

# Get last base64 encoded part of the URL
def get_last_base64_part(url):
    parts = url.split("/")
    last_part = parts[-1]
    if last_part:
        try:
            decoded = base64.b64decode(last_part)
            return decoded.decode('utf-8')
        except Exception as e:
```

```
            pass
    return None
# Import URLs from addresses.csv or use the local wordlist
def import_urls():
    if os.path.exists('addresses.csv'):
        with open('addresses.csv', 'r') as csvfile:
            reader = csv.reader(csvfile)
            urls = [item.strip() for row in reader for item in row]
            return urls
    else:
        return ["https://example1.se", "https://www.example2.com"]
# List wiht texts/URLs for generating QR codes
text_list = import_urls()

# Loading GIF (only once)
loading_filename = 'loading.gif'
create_loading_gif(loading_filename, duration=15)

# Separate final animation files for each URL from the lists
for index, text in enumerate(text_list):
    qr_filename = f'qr_{index}.gif'
    create_static_qr_gif(text, qr_filename, duration=75)

    # Base64 or domain in filename
    domain_name = get_domain_name(text)
    last_base64_part = get_last_base64_part(text)
    file_name = domain_name if domain_name else last_base64_part
    output_filename = f'final_animation_{file_name}_{index}.gif'

    # Merge loading and static
    with imageio.get_writer(output_filename, mode='I', duration=50) as writer:
        loading = imageio.get_reader(loading_filename)
        for frame in loading:
            writer.append_data(frame)

        qr = imageio.get_reader(qr_filename)
        for frame in qr:
            writer.append_data(frame)
```

Appendix D

Skadlig	Blockerat URL klartext	Gen miniatyr	Blockerat statisk bild	Blockerat QR-animation	Korrekt QR	Phishtank.org ID	VirusTotal.com	URL	Eset Premium blockerat	Trend Micro QR scanner blockerat	Kaspersky app blockerat
JA	JA	JA	JA	NEJ	JA	8479272	4	https://uspz.usspaod.to	JA	JA	JA
JA	JA	NEJ	JA	NEJ	JA	8479041	5	https://d8ge5f.ru.net/Q	JA	JA	NEJ
JA	JA	NEJ	JA	NEJ	JA	8479067	14	https://loginaccount99.x	NEJ	JA	JA
JA	JA	NEJ	NEJ	JA	NEJ	8479115	11	https://help-supporting	JA	JA	JA
JA	NEJ	NEJ	NEJ	NEJ	JA	8479141	9	https://www.cayxhecb.c	NEJ	JA	JA
JA	NEJ	NEJ	NEJ	NEJ	JA	8479304	4	https://adobe-pd.pages	NEJ	JA	JA
JA	JA	NEJ	JA	NEJ	JA	8478766	11	https://attmailerinnfos.	JA	JA	JA
JA	NEJ	NEJ	NEJ	NEJ	JA	8478720	7	http://appis-terra-supu	NEJ	JA	JA
JA	JA	NEJ	JA	NEJ	JA	8478716	11	https://154.235.205.92.h	JA	JA	JA
JA	JA	NEJ	JA	NEJ	JA	8478672	12	https://g81ykq.webwavv	NEJ	JA	JA
JA	NEJ	JA	NEJ	NEJ	JA	8478668	4	https://sites.google.com	JA	JA	NEJ
JA	NEJ	JA	NEJ	NEJ	JA	8478650	4	https://exoduetkogin.gi	NEJ	JA	JA
JA	NEJ	JA	NEJ	NEJ	JA	8475346	21	https://fee-67b.pages.d	JA	JA	JA
JA	NEJ	NEJ	NEJ	NEJ	JA	8478561	16	https://streaming-yatco	JA	JA	JA
JA	NEJ	NEJ	NEJ	NEJ	JA	8479833	12	https://vpdoi.pages.dev	JA	JA	JA
JA	JA	NEJ	JA	NEJ	JA	8479854	21	https://cloudflare-ipfs.c	JA	JA	JA

Skadlig	Blockerat URL klartext	Gen miniatyr	Blockerat statisk bild	QR-animation	Korrekt QR	Fortune 500 nr.	VirusTotal.com	URL	Eset Premium blockerat	Trend Micro QR scanner blockerat	Kaspersky app blockerat
NEJ	NEJ	NEJ	NEJ	NEJ	JA	1	0	https://www.walmart.co	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	3	1	https://www.amazon.co	NEJ	NEJ	NEJ
NEJ	NEJ	JA	NEJ	NEJ	JA	8	0	https://secure6.store.ap	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	10	0	https://www.healthsafe	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	11	0	https://www.cvs.com/a	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	15	0	https://identity.vwgrou	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	18	0	https://mscs.mckesson.c	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	25	0	https://account.samsung	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	26	0	https://signin.costco.co	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	27	0	https://www.foxconn.co	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	28	0	https://mybank.icbc.co	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	29	0	https://ibsbistar.ccb.co	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	30	1	https://login.live.com/lc	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	34	0	https://market.cardinalh	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	35	0	https://my.cigna.com/w	NEJ	NEJ	NEJ
NEJ	NEJ	NEJ	NEJ	NEJ	JA	40	0	https://login.valero.com	NEJ	NEJ	NEJ

blått = MDO

Fig. 58. Utfall Experiment 1 – gif animeringar i MDO developer sandbox och data från alla verktyg som testades.