Förstå phishing-simulering
medvetenhet bortom klickfrekvens

Insikter från

JUNGLEMAP

april 2024

JUNGLEMAP

Innehåll

Introduktion

Fler och fler av Junglemaps kunder använder phishingsimulering som en integrerad del av sin utbildning i informationssäkerhet med en 47 % ökning av antalet aktiviteter och en 57 % ökning av antalet kunder mellan 2022 och 2023.

Det här kommer inte som någon överraskning. Phishing är fortfarande en av de vanligaste formerna av attacker och vi människor är fortfarande den primära måltavlan. Samtidigt utvecklas tekniken för phishingattacker hela tiden, och hotaktörerna hittar ständigt nya vägar att ta sig in. Detta i sig är ett starkt argument för fortsatt phishingsimulering, som en integrerad del av utbildningen i informationssäkerhet.

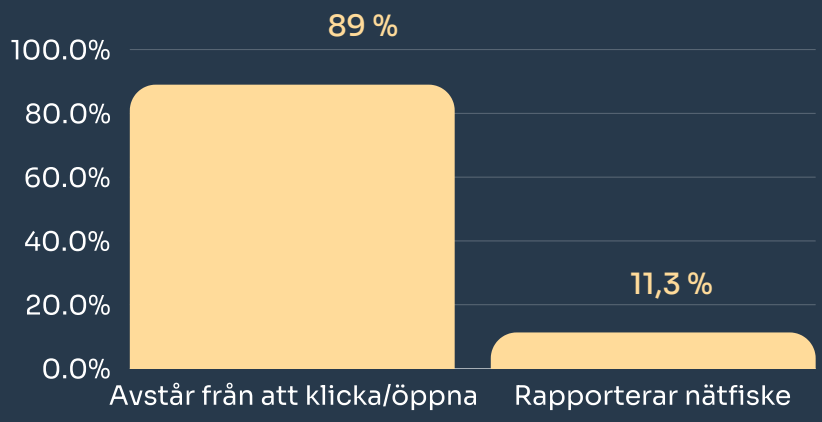
De flesta phishingsimuleringar fokuserar på resultaten här och nu, istället för att leverera långsiktiga beteendeförändringar. Det beror i grunden på det felaktiga antagandet att det räcker med phishingsimuleringar och uppföljande utbildning under en kortare period. Men den här typen av upplägg har visat sig vara verkningslösa på lite längre sikt. Baserat på aggregerad användardata ser vi att konsekvent upprepning och förstärkning är nyckeln i all utbildning i som syftar till att öka medvetenheten i cybersäkerhet.

Men det finns också andra slutsatser att dra: Enbart phishing-simulering räcker inte. Det måste vara en del av ett större sammanhang med medvetenhet om cybersäkerhet. Dessutom bör syftet med ett phishingsimuleringar inte vara att få en klickfrekvens på noll procent. Effekten blir större om simuleringarna ger utrymme för lärande och fokuserar på organisationens framgångsfaktorer bortom klickfrekvensen.

Bortom klickfrekvensen

Ett misslyckande i en phishingsimulering ska fungera som en väckarklocka. Och det är vad som händer efter uppvaknandet som är det viktigaste. De flesta är såklart försiktigare efter att ha klickat i en phishingsimulering, men de medarbetare som upprepade gånger gör misstaget är sannolikt medarbetare med högre riskprofil, vilket både kan bero på individens beteende, men lika ofta på yttre faktorer som arbetsbelastning och stress. Medarbetare med högre riskprofil kan har stor nytta av intensifierad träning och simuleringar.

Men den viktigaste frågan är den här: Vad leder phishingsimulering till? Enligt Microsoft Digital Defense Report rapporterar bara 11,3 % av användarna som får phishing-mail om dem, trots att 89 % avstår från att klicka på länkar eller öppna bilagor.



Det här gapet visar hur viktigt det är att all phishingsimulering måste vara en del av ett större utbildningsammanhang om cybersäkerhet. Det viktiga är inte bara klickfrekvensen, utan snarare vad som händer härnäst. En phishingsimulering utförd i en organisation med en god cybersäkerhetskultur där alla anställda uppmanas att rapportera och veta hur man gör detta, kommer simuleringarna att få mycket större effekt.

“Att inte klicka är bättre än att klicka, men rapportering är ännu viktigare.”

Phishing-simulering enligt Junglemap

På Junglemap uppmuntrar vi våra kunder att använda phishingsimulering som en integrerad del av deras övergripande utbildning i informationssäkerhet och att fokusera på hur man skapar en bättre förståelse för organisationernas cyberhygien.

2006 uppfann vi NanoLearning och har sedan dess nått över 7 miljoner slutanvändare. Baserat på aggregerad användardata rekommenderar vi alltid våra kunder att distribuera våra 3-minuters NanoLearning-lektioner var tredje vecka under hela året. Helt enkelt för att bekämpa den så kallade glömskekurvan och skapa långsiktiga beteendeförändringar när det gäller säkerhet.

Alla som försöker uppnå en långvarig medvetenhet och vaksamhet när det gäller phishing bör sträva efter samma typ av frekvens. Detta skapar inte bara rätt inlärningstakt, utan hjälper också till att undvika så kallade simulerings-trötthet, orsakad av överanvändning av phisingsimulering.

Att hitta rätt balans mellan hög frekvens, att undvika simuleringströtthet och att samtidigt nå rätt målgrupp med relevanta ämnen är en utmaning i sig. Med phishingsimulering från Junglemap kan våra kunder enkelt hantera och finjustera sina simuleringar genom att välja frekvens, typ av phishingteknik, bransch och roll – och sedan matcha dessa inställningar med rätt mallar från vårt bibliotek med över 170 färdiga phishingmallar.

Genom att göra detta kommer personer inom HR att få simulerade phisingmail om HR-relaterade frågor, personer inom ekonomi om finansiella frågor, etc, etc. Noggrannheten i den här typen av riktade och svårupptäckta simuleringar kommer att skapa ökad medvetenhet på varje avdelning, samt ett organisatoriskt lärande mellan olika avdelningar.

"Phishing-simulering bör behandlas som brandövningar", säger en av Junglemaps Customer Success Managers som hjälper kunder att få ut det mesta av sina simuleringar. "Det kommer inte att ge någon effekt om simuleringen slutar med att individen lär sig att inte klicka, men inte delar den insikten med andra."
När jag ger organisationer råd om hur de ska följa upp testerna ber jag dem alltid se bortom siffrorna och istället fokusera på:

- Hur lång tid tog det innan din IT-säkerhet fick den första rapporten?
- Hur lång tid tar det att analysera detta och informera resten av organisationen?
- Har du rätt kommunikationsverktyg och kanaler på plats för detta?

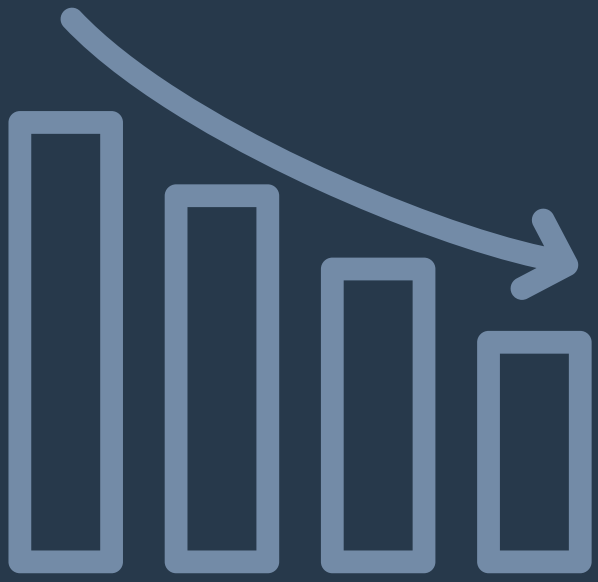
I flera år har vi arbetat med att ge organisationer från olika branscher råd om hur de ska använda phishingsimulering för att passa organisationens syfte. När vi gör detta försöker vi alltid vägleda genom denna lista:

1. Sätt tydliga lär- och effektmål
2. Samarbeta mellan avdelningar inom organisationen
3. Utbilda anställda om phishingattacker innan du genomför en simulering
4. Övervaka och spåra resultat och följ upp med anställda genom chefsledet
5. Samla insikter från simuleringsrapporterna
6. Uppdatera och anpassa phishingsimuleringar kontinuerligt
7. Upprepa simuleringarna regelbundet
8. Använd simuleringsresultaten som underlag för säkerhetspolicyer

Trovärdiga resultat – inte förenklade framgångssagor

Många leverantörer av phishingsimulering använder framgångssagor baserade på imponerande och förvånansvärt linjära förbättringar i sin historiska användarstatistik. Vi uppmanar att alla organisationer som letar efter ett simuleringsverktyg bör ifrågasätta grafer som denna.

Naturligtvis har vi många exempel på stadiga framsteg och förbättrade siffror. Men att bara upprepa samma övning om och om igen skapar inte den medvetenhet som behövs när hotbilden ständigt förändras med hotaktörer som använder AI-drivna phishingattacker som blir mer och mer sofistikerade och svårare att upptäcka.



Vad är ett bra resultat?

Det här väcker en annan viktig fråga: Vad är ett bra resultat? I teorin vill de flesta som är ansvariga för cybersäkerheten komma så nära en klickfrekvens på noll procent som möjligt. Men att bara sikta på låga siffror tillåter inte organisationen att träna och vara beredd på det som är viktigare: nya typer av hot som de anställda ännu inte har stått inför.

Syftet med phishingsimulering bör inte vara att få en klickfrekvens på noll procent, utan att utbilda användare att känna igen nya taktiker, tekniker och tillvägagångssätt som används av angriparna. Med det i åtanke uppmuntrar vi alltid våra kunder att sikta på mål som erbjuder en marginal för lärande och fokusera på framgångsfaktorer och på mätvärden utöver klickfrekvenser.

Förändra beteenden genom organisatoriskt lärande

Enligt flera rapporter börjar branschen för säkerhetsmedvetenhet och utbildning nu att prioritera beteendeförändring framför informationsleverans. Genom att använda NanoLearning som en metod för att förändra beteenden välkomnar vi detta tillvägagångssätt eftersom det är detta som i slutändan skapar motståndskraftiga säkerhetskulturer.

Men där många leverantörer fokuserar på individuella skillnader och individanpassad träning, menar vi att företag måste lägga mer fokus på organisatoriska förändringar och beteenden. Även om många av våra kunder använder vår phishingsimulering genom att rikta in sig på olika kategorier av anställda med olika typer av phishingmallar, betonar vi alltid hur viktigt det är att skapa ett organisatoriskt lärande mellan olika grupper av anställda. Återigen, minst lika viktigt som att inte klicka, är att ha en chans att dela insikter om varför du inte klickade.

Exempel

Phishingsimuleringar används på många olika sätt

Phishingsimulering med Junglemap syftar alltid att hjälpa till att bygga en säkerhetskultur och stärka de mänskliga brandväggarna. Men organisationer skiljer sig åt och befinner sig i olika stadier i sin säkerhetsmognad. Här är några fall som visar hur olika organisationer använder vår simulering på olika sätt, men med samma mål: Att öka medvetenheten på organisationsnivå.

1. Phishingsimulering för att öka medvetenheten – om medvetenhet

Ett byggföretag använder Junglemaps phishingsimulering ganska intensivt som ett sätt att påminna om vikten av den ordinarie och regelbundna utbildningen i informationssäkerhet. De gör det genom att starta nya utbildningar i informations-säkerhet med ett phishing-test – vilket ofta ger ganska höga klickresultat **(19 %)**

– Medvetenheten om behovet av mer medvetenhet ökade. I slutet av kursen med samma målgrupp klickade bara **1,3 %** även om svårighetsgraden var högre på det andra testet.

2. Förstå beteendet hos den som inte klickar

En kommun har kämpat med låga grader av slutförande i sin övergripande utbildning i informationssäkerhet. Detta återspeglades också i resultaten av phishingsimuleringarna, där många anställda inte märkte simuleringarna alls, vilket ledde till en klickfrekvens på 1,3 och 0,6% i två tester. För att få en bättre förståelse för organisationens säkerhetsbeteende riktades mer uppmärksamhet mot de som öppnat phishing-mailen, men inte klickat och hur de agerade efter att ha upptäckt phishing-e-posten. Rapporterade de, fick de den uppmärksamhet som behövdes av sina närmaste chefer? Ökade de medvetenheten för phishingsimulering i sina team? Den här typen av frågor gav organisationen en mycket bättre förståelse framöver.

3. Kickstartande nybörjare

Ett kommunägt kollektivtrafikföretag introducerade sin utbildning i cybersäkerhet med Junglemap i november 2022 och implementerade sin första nätfiskesimulering i maj 2023. Detta med vetskapen om en låg initial medvetenhet i säkerhetsfrågor.

Även om phishingsimuleringen definierades som enkel att genomskåda var det **43 % av mer än 1.400 anställda som klickade på länken donotclick.net.**
Detta var givetvis en väckarklocka för organisationen och ett starkt argument för att fortsätta med utbildning i informationssäkerhet. Detta i kombination med kommunikation kring informationssäkerhet genom chefsleden i organisationen.

Fem månader senare genomförde samma organisation en ny simulering, med en mer sofistikerad phishingmall med ett uppdaterat innehåll och ett verklighetsförankrat budskap. Nu hade dock klickfrekvensen **sjunkit till 19 %.**
En enorm förbättring tack vare olika insatser för att öka medvetenheten, men fortfarande ett högt antal jämfört med organisationens egna förväntningar.

4. Hålla dina anställda på tårna

Ett medelstort bilföretag bestämde sig för att använda phishing-simulering ganska ofta för att hålla sina anställda "på tårna". Detta har resulterat i en betydligt högre uppmärksamhetsnivå, vilket också återspeglas i de förbättrade resultaten mellan den **första simuleringen (27,5 %)** och **den sista (20 %).** Eftersom detta i grund och botten är vad företaget vill uppnå, har de också beslutat att fortsätta använda frekventa tester framöver.

5. Kontinuerlig förbättring

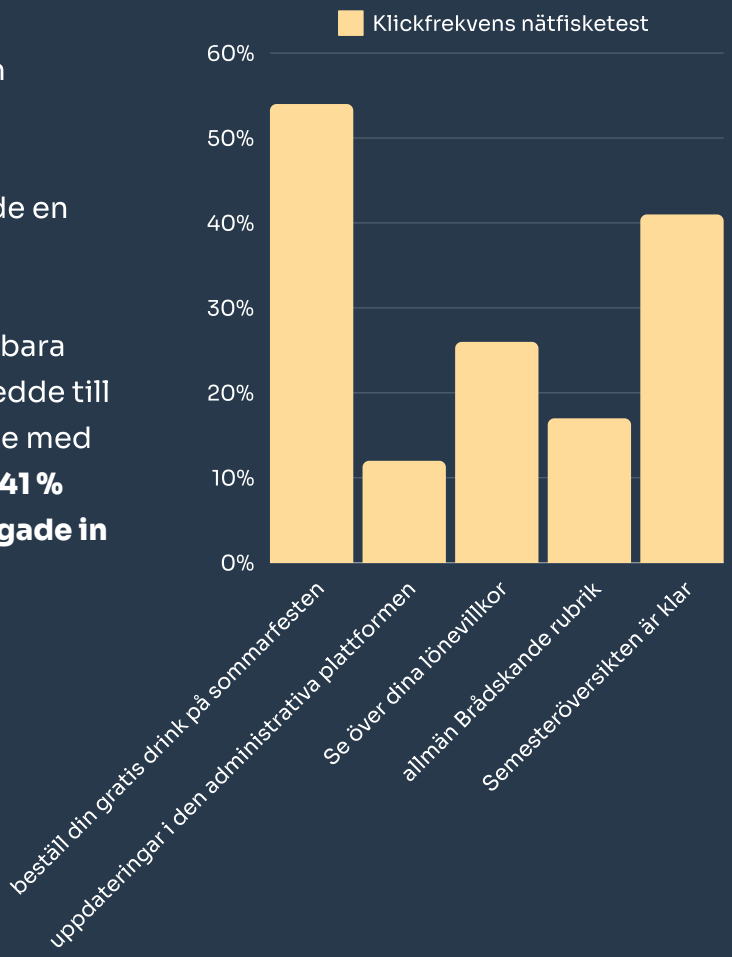
En starkt digitaliserad organisation som genomför en kontinuerlig utbildning i informationssäkerhet med Junglemap genomför phishingsimulering två gånger om året. I maj 2023 hade de en klickfrekvens på **16,2 %** på en svår nivå med skräddarsytt innehåll och varumärkesmallar.
Med sin andra simulering nådde de en klickfrekvens på **11,6 %**. Fortfarande långt över "skolbokssiffrorna", men för denna organisation ett tydligt tecken på att gå i rätt riktning mot sina egna mål om "ständiga förbättringar".

6. Olika triggers – olika resultat

Vi ser också stora skillnader i klickfrekvenser enbart beroende på själva ämnet och tajmingen. Att be de anställda på en mansdominerad arbetsplats att anmäla sig till julfesten med ett budskap att ”om du inte anmäler dig får du automatiskt det vegetariska alternativet” – resulterar i fler klick. Liksom versionen med "beställ din gratis drink på sommarfesten". **(54 % klickfrekvens)**

Detta kan tyckas vara lätta knep, men det speglar verkligen ett mönster som vi ser i många fall. Klickfrekvensen beror regelbundet på två faktorer: avsändarens och ämnets trovärdighet och direkta effekter för mottagaren på ett personligt plan.

När de anställda på ett nordiskt konsultföretag fick phishing-mejl om "uppdateringar i den administrativa plattformen", **klickade endast 12 %,** men när phishing-mejlet istället gällde en "Översyn av dina lönevillkor", **så klickade 26 %.**
Samma tendens när phishing-mejlet bara hade en allmänt hållen rubrik, vilket ledde till en **klickfrekvens på 17 %**, i jämförelse med "Semesteröversikten är klar" med en **41 % klickfrekvens** och där även **75 % loggade in** på den falska inloggningssidan.



Sammanfattning

Baserat på lång erfarenhet från rådgivning kring phishingsimulering i en mängd olika organisationer är detta de viktigaste lärdomarna för oss på Junglemap.

- Konsekvent upprepning och förstärkning är nyckeln i all utbildning i säkerhetsmedvetenhet. Detta är också ett starkt argument för kontinuerliga nätfiske-simuleringar.
- Enbart nätfiske-simulering räcker inte. Det måste vara en del av ett större sammanhang med medvetenhet om informations- och cybersäkerhet.
- Sikta på trovärdiga resultat – inte förenklade framgångssagor. Syftet med phishingsimulering bör inte vara att få en klickfrekvens på noll procent. Det måste erbjuda en marginal för lärande och sätta fokus på mätbara framgångsfaktorer utöver klickfrekvenser.
- Lika viktigt som att inte klicka, är att ha en chans att dela insikter om varför du inte klickade med ditt team.

Källor

- Microsoft Digital Defense Report 2023 https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
- Gone phishing-turnering (Terranova Phishing Benchmark Global Report 2022) Medsponsrad av Microsoft
- SlashNext-State of Phishing Report 2023
- Nätfiske i organisationer: Resultat från en storskalig och långtidsstudie (Lain, Kostiainen, Capkun, ETH, Zürich 2021)

Kontakt

Läs mer och kontakta oss för mer information om hur vi använder nätfiskesimulering i vår utbildning om informationssäkerhet.

Varning:
Vi förfalskar inte! Vi använder aldrig några varumärken eller logotyper från tredje part utan samtycke.