

Cybersikkerheds-awareness-træning for store organisationer



Seks almindelige faldgruber, der skal undgås, når man uddanner tusindvis af medarbejdere med cybersikkerheds-awareness-træning



De seks bedste metoder til vellykket cybersikkerhed-awareness-træning for store organisationer



MetaCompliance®



Seks almindelige faldgruber, der skal undgås, når man uddanner tusindvis af medarbejdere med cybersikkerheds-awareness-træning



1 Den samme gamle historie for alle

Ikke alle phishing-kampagner er ens. Rollebaseret phishing bruges i spear-phishing og sofistikerede social-engineering-svindelnumre. Afgrænsning af roller i større organisationer betyder, at cybersikkerheds-awareness-træning også bør have et rollebaseret fokus. Ved at skræddersy awareness træning og phishing-simuleringsøvelser til at passe til de typer angreb, der fokuserer på specifikke roller, f.eks. administrerende direktører og kreditorerne, er der større sandsynlighed for, at uddannelsen forbliver relevant og fokuseret. Når det drejer sig om awareness-træning, vil en ensartet tilgang sandsynligvis efterlade mange sårbarheder i hele organisationen.

Et vigtigt aspekt af enhver form for awareness-træning, herunder den rollebaserede version, er at uddele materiale der har fokus på konteksten efter en simuleret phishing-kampagne. Awareness-træning er mest effektivt, når medarbejderne forstår hvorfor og af hvilken grund den skal finde sted. Sørg for at tilbyde supplerende awareness-træning for at sikre, at målet med den simulerede phishing-øvelse er forstået.

2 Kedelige sikkerhedsuddannelsesmoduler og inkonsekvent cybersikkerheds-awareness-træning

Gør awareness-træningen engagerende og mindre kedelig. Enhver form for awareness-træning, herunder om cybersikkerhed, har større sandsynlighed for at blive en succes, hvis kursisterne er interesserede i det materiale, der anvendes, og hvis dette materiale er relevant.

Gør uddannelsesmodulerne sjove og underholdende ved at bruge et varieret indhold. Interessante og engagerende videospil er vindere blandt medarbejderne. Du kan bruge spoofs fra kendte shows til at skabe videoserier i Line-of-Duty stil, der gennemgår sikkerheds-scenarier for at øge interessen og engagere medarbejderne. Cybersikkerheds-måned finder sted hvert år i oktober.^[1] Nogle organisationer kan godt lide at lave særlige videoer og **plakater** til cybersikkerheds-awareness-træning, der falder sammen med årets tema, f.eks. var temaet i 2021 "Tænk, før du klikker".

Konsistens er desuden et vigtigt aspekt af menneskelig adfærd. Konsistens er med til at skabe bånd og tillid, og det er en måde, hvorpå mennesker kan opbygge mentale modeller, som de kan stole på. Der er derfor større sandsynlighed for, at regelmæssig uddannelse, der følger genkendelige og engagerende moduler, vil lykkes.^[2]



3 Uddannelsesmateriale, medarbejderne ikke kan relatere til, og sproglige problemer

En vellykket form for cybersikkerheds-awareness-træning er en interaktiv oplevelse. Brugen af "point-of-need" læringsoplevelser sikrer, at medarbejderne får instruktioner om, hvor de fejlede, og hvordan de kan rette op på det på det punkt, hvor der sker en farlig interaktion med en phishing-besked eller et andet simuleret angreb.

Et andet vigtigt aspekt ved at skabe relaterbart awareness materiale er at forbinde uddannelsen med aktuelle begivenheder. F.eks. blev der under COVID-19-pandemien lavet store phishing-e-mailkampagner, der efterlignede e-mails fra Verdenssundhedsorganisationen (WHO) og brugte brandet til at narre offentligheden. For nylig er krigen i Ukraine blevet brugt på en lignende måde, idet cyberkriminelle har lavet svindelnumre, hvor de lader som om, at de indsamler midler til Ukraine. ^[3]

For multinationale organisationer med hubs, operationer eller kontorer over hele verden er det en stor udfordring at lave kampagner på brugernes modersmål. Alt for ofte er leverandører afhængige af dårligt oversat indhold og brugerautomatiserede værktøjer, der ikke tager højde for subtile forskelle i den lokale kultur. Hvis en medarbejder ikke forstår uddannelsen fuldt ud, kan man ikke forvente, at han/hun følger den.



4 Fanget i det samme cyberangrebsmønster

Landskabet for cybersikkerhedsangreb er aldrig statisk. Cyberkriminelle ændrer hele tiden teknikker og taktikker for at gøre deres cyberangreb vellykkede. Brug den samme tankegang, men vær ikke bange for at rette til, efterhånden som landskabet for cybertrusler ændrer sig. Justér dine simulerede phishing-kampagner, tilføj nye cyberangrebstaktikker i uddannelsen, og sørg for, at uddannelsen passer til den type angreb, der anvendes mod større organisationer.

5 Hvem er ansvarlig for uddannelsen?

Det er en udfordring, som kan give anledning til intern debat. Hvem skal stå for uddannelsen? IT eller HR? Cybersikkerheds-awareness-træning er ikke en engangsforestilling. Den skal gennemføres regelmæssigt, der skal foretages analyser af resultaterne, og der skal tilbydes støtte til medarbejdere og "vaneforbrydere", som har svært ved at tage uddannelsen til sig. Samarbejde om udformning og styring af cybersikkerheds-awareness-træning kan være den rigtige løsning til din organisation. Det kan være en fordel at anvende specialiserede tredjeparter til at håndtere awareness-træningen og levere den "know-how", der skal sikre, at den bliver en succes.

6 Fortrolighed ved hændelsesrapportering

Medarbejderne skal føle sig trygge nok til at rapportere en sikkerhedshændelse. Større organisationer skal arbejde på trygheden og tilskynde til rapportering af hændelser for at sikre, at it-teams har tid og de rette oplysninger til at reagere på en trussel.



De seks bedste metoder til vellykket cybersikkerheds-awareness-træning til store organisationer

Hvad hvis din organisation er en større organisation med mange medarbejdere i flere forskellige brancher og afdelinger, hvor mange medarbejdere arbejder eksternt, rejser eller arbejder på hjemmekontor? Hvordan uddanner du dine medarbejdere i stor skala for at have styr på sikkerheden?

Hvis derudover er et stort økosystem af forsyningskæder, både som leverandør og forbruger af forsyninger, har du en situation, som en cyberkriminell kan udnytte. Vejen frem med cybersikkerheds-awareness-træning i stor skala er at bruge følgende seks principper for bedste praksis.



1 Sæt et lokalt præg på awareness træningen på tværs af afdelinger og filialer

Lav cybersikkerheds-awareness-træningsprogrammer, der passer til din egen organisationsstruktur. Planlæg dine awareness-kampagner, så de når ud til alle dele af dit organisationsdiagram. Sæmstensæt disse programmer, så de afspejler rollerne i de afdelinger, der er udsat, og etabler skræddersyet awareness-træning om disse risici.

MetaCompliance leverer uddannelse på 35 forskellige sprog og snart vil endnu flere sprog blive understøttet. Disse sprogversioner er alle udarbejdet af indfødte, der taler modersmålet for at sikre, at oversættelsen er korrekt. På alle de understøttede sprog tilbyder MetaCompliance alt vores eLearning-indhold med sproglig korrekt lyd og undertekster.

2 Gør det personligt, og få det til at blive husket

Personaliseret cybersikkerheds-awareness-træning afspejler i højere grad den virkelige brug af spear-phishing. Personlige awareness-træningsprogrammer kan konfigureres ved hjælp af avancerede sikkerhedsuddannelsesplatforme. Disse systemer kører skræddersyede **phishing-simuleringer** og andre sikkerhedsuddannelses-moduler, der nøje afspejler den personlige situation for en given medarbejder. Der skal desuden sørges for, at uddannelsen personliggøres og brandes som din egen. Hvis medarbejderne kan se, at uddannelsen er iværksat af den organisation, de arbejder for, er de mere tilbøjelige til at tage den til sig.



3 Korte uddannelsessessioner

Regelmæssig uddannelse med materiale og moduler i små bidder er en vellykket strategi for cybersikkerheds-awareness-træning. De korte uddannelsessessioner forhindrer uddannelsestræthed. Igen, det er ideelt at have disse korte moduler på en række forskellige sprog i store organisationer, der kan have mange flersprogede medarbejdere rundt om i verden.



4 Automatisér cybersikkerheds-awareness-træning med detaljeret rapportering

Ved at automatisere dit **cybersikkerheds-awareness-træningsprogram** skaber du en mere effektiv uddannelsesproces og frigør samtidig en stor del af din tid. Fordelene ved automatiseret cybersikkerheds-awareness-træning er bl.a., at du hurtigt kan skalere din træning uden yderligere ressourcer, og du kan planlægge en årlig kampagne for at sikre kontinuerlig læring hele året rundt. Desuden kan du med den detaljerede og sofistikerede rapportering, der følger med en automatiseret platform, se, om der er et højt engagement blandt medarbejderne.

5 Gør cybersikkerheds-awareness-træning konsistent og regelmæssig

Mange organisationer undlader regelmæssig cybersikkerheds-awareness-træning i løbet af året. Automatiseret cybersikkerheds-awareness-træning skaber en engagerende læringsoplevelse for medarbejderne hele året rundt, hvilket sikrer, at cybersikkerhedsstrusler forbliver i hukommelsen. Automatiseret awareness-træning der anvender en "indstil det og glem det"-tilgang, hjælper med at spare tid og ressourcer. Det er en proaktiv og organiseret måde at gennemføre effektive uddannelsesprogrammer på i stedet for at håbe på, at det vil være nok med en ad hoc-tilgang til awareness-træning.

6 Giv din bestyrelse et "investeringsafkast" (Return on Investment – ROI)

Det er yderst vigtigt at måle et programs succes for at afgøre, om det er vellykket eller ej, men ledere inden for sikkerhed og risikostyring kæmper alligevel tit med at retfærdiggøre deres organisations investering. Budgetterne er stramme, og det er vigtigt at bevise, at cybersikkerheds-awareness-træning virker. Ved at bruge en platform med en rapporteringspakke, der opsamler data fra de tusindvis af medarbejdere, der gennemfører awareness-træningen, kan du bevise, at compliance-forpligtelserne er opfyldt, påvise forbedringer i cybersikkerhedsrelateret adfærd og vigtigst af alt, give din bestyrelse et investeringsafkast (ROI).

Konklusion

En afsluttende udtalelse fra en **(ISC)²rapport** opsummerer situationen med hensyn til cybersikkerheds-awareness-træning:^[4]

“ Manglende cybersikkerheds-awareness og færdigheder blandt alle medarbejdere er fortsat den **største sikkerhedsrisiko for organisationer**. Cybersikkerhedseksperter er enige om, at **6 ud af 10 medarbejdere ville have gavn af sikkerhedsuddannelse og/eller certificering** i forbindelse med deres arbejde for at opfylde dette behov for awareness og færdigheder. ”

Hvis man går et skridt videre, er det vigtigt at give medarbejderne redskaberne til at beskytte sig selv og deres organisation, men det skal gøres for at opnå det bedst mulige resultat. Cybersikkerheds-awareness-træning i stor skala er ikke nogen nem opgave i sig selv. En masseuddannelse af medarbejdere på ethvert område er kompleks, men cybersikkerhed kan være et tørt og kedeligt emne, som let kan miste publikum, hvis det gøres forkert. Ved her at følge de seks bedste fremgangsmåder og undgå de problemer, der opstår ved dårlig cybersikkerheds-awareness-træning, kan selv de største og mest fordelte organisationer holde cyberkriminalitet ude.

Problemer kan bane vej for bedste praksis! Her er seks vigtige ting, du skal gøre for at sikre, at din cybersikkerheds-awareness-træning fungerer.

Opsummering – Tjekliste

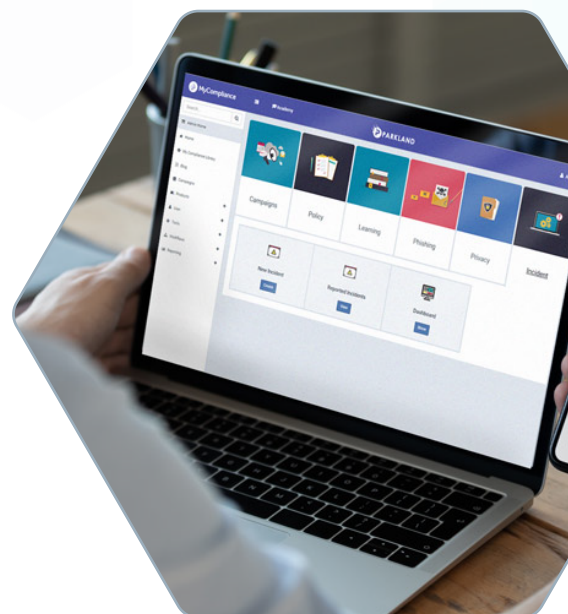
- ✓ Spar tid, og styrk organisationens modstandsdygtighed ved at engagere medarbejderne med automatiseret cybersikkerheds-awareness-træning hele året rundt.
- ✓ Personliggør cybersikkerheds-awareness-træningen og indarbejd en række forskellige stilarter og formater for at fange slutbrugernes opmærksomhed.
- ✓ Skab skræddersyet og målrettet cybersikkerheds-awareness-træning, der er specifik for din organisations behov og kultur.
- ✓ Servér cybersikkerheds-awareness-træningen i korte, letfordøjelige portioner for at undgå brugertræthed.
- ✓ Brug rapportering til at dokumentere, at lovkrav er opfyldt og bevise, at programmet for cybersikkerheds-awareness forbedrer slutbrugernes adfærd.
- ✓ Øg medarbejdernes engagement, gennemførelsesprocent og fastholdelse med lokalt tilpasset indhold.

MetaCompliance er med sine 15 års erfaring og med velkendte kunder over hele verden specialister, når det gælder levering af cybersikkerheds-awareness-træning på organisationssniveau. Vi ved, hvad det kræver at levere effektiv uddannelse til tusindvis eller endda titusindvis af medarbejdere.

Prøv os af og se, om det passer –
bed om en demo i dag.

✉ **info@metacompliance.com**

🌐 **www.metacompliance.com**



Kildereferencer

- [1] <https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month>
- [2] <https://www.routledge.com/Consistency-in-Cognitive-Social-Behaviour-An-Introduction-to-Social-Psychology/White/p/book/9781138851214>
- [3] <https://www.bbc.co.uk/news/technology-60836962>
- [4] <https://www.isc2.org/Research/Workforce-Study>