Tjekliste til Phishing simuleringer

Her er vores anbefalinger til, hvad du kan gøre før, under og efter enhver phishing kampagne.

Før simuleringen – Forbered dig selv og din organisation

Hvis det er jeres første kampagne

- Vi anbefaler, at du kommunikerer ud til din organisation, at I vil udføre phishing-træning, og at du vil have adgang til at se resultaterne. Du kan finde en skabelon til dette **her.**
- Mind din organisation om, hvor de kan finde passende sikkerhedsprocedurer. Genopfrisk deres hukommelse om processen for phishing/mistænkelige e-mails.
  - Har I ikke en klar proces? Træningen vil hjælpe dig til at identificere, hvilke områder der har brug for opmærksomhed.

Før hver phishing-kampagne

- [ ] Fortæl dem, der ville kunne lukke ned for et rigtigt angreb, at I laver en test, og at de skal lade det gå sin gang
- [ ] Sæt mål for din organisation. Skriv ned, hvordan du tror, de vil klare sig i kampagnen.
- [ ] Planlæg, hvordan du vil reagere. Vi anbefaler, at du opfører dig normalt under simuleringen. Prøv at holde et pokerface. Din reaktion vil påvirke, hvor alvorligt din organisation ser på phishing-truslen.
  - Det kan være en god idé at give positiv forstærkning, når medarbejderne gør det rigtige. Tak dem for at gøre opmærksom på e-mailen og bruge den rigtige rapporteringsprocedure.
- [ ] Hvis du ikke er på kontoret på kampagnedagen, hvordan vil du måle responsen? Måske skal du udpege en kollega til at hjælpe dig med at registrere, hvordan det gik på kontoret.
- [ ] Husk at whiteliste
- [ ] Bekræft, at du har modtaget testmailen, og at linksene fungerer som aftalt.

På dagen for phishing-simuleringen

Hvad bør du observere og notere

- Samtaler på kontoret
  - # _____ indlæg omkring e-mailen på interne kommunikationskanaler (f.eks. Teams, slack, e-mail, uformelle samtaler ved kaffemaskinen).
- Rapportering af e-mailen – hvem rapporterer, hvordan og under hvilke omstændigheder?
  - # _____ medarbejdere, der rapporterede e-mailen korrekt (efter jeres procedure).

CyberPilot

- Hvad er deres reaktion? (Tager de det seriøst, ser de det som endnu en "test", ignorerer de det, osv.)

  # _____ af åbenlyst ***positive*** holdninger, du kan observere til phishing-træningen.

  # _____ af åbenlyst ***negative*** holdninger, du kan observere til phishing-træningen.

- Reaktionstid

  _____ Den tid, det tog for IT-chefen eller den ansvarlige at blive advaret om phishing-forsøget.

  _____ Tid fra e-mailen blev sendt, til hele organisationen blev gjort opmærksom på det.

Hvad skal gennemgås på platformen (metrikker fra simuleringen)

På platformen kan du se datapunkterne fra din kampagne, som de kommer ind.

- Klikrate på link.
- Konverteringsrate (dataindsendelser).

Efter phishing-simuleringen

- [ ] Del resultaterne. **Her er der en skabelon, som du kan bruge til inspiration.**
  - Del de overordnede resultater og tegn på phishing med organisationen på et generelt niveau.
  - Kontakt straks dem, der faldt for testen, for at dele feedback.
- [ ] Giv yderligere træning til de brugere, der har brug for det. **Se vores artikel om, hvordan du tilmelder kurser til specifikke brugere.**
- [ ] Anerkend brugere, der regelmæssigt rapporterer simulerede (og ægte) phishing
- [ ] Analysér resultaterne, og identificer områder, der kan forbedres.

  Hvordan klarede medarbejderne sig? Hvor effektiv er den eksisterende rapport-eringsprocedure?