Do’ś en don'ts voor een succesvolle phishing-campagne

Phishing is een van de grootste dreigingen voor organisaties op het gebied van cybersecurity. Iedereen heeft waarschijnlijk wel eens een phishingmail ontvangen. Sommige mails zitten beter in elkaar dan anderen. Door medewerkers bewust bloot te stellen aan een nepaanval, leren ze verdachte mails herkennen voordat het echt fout gaat. Maar wat maakt een phishing-campagne leerzaam en succesvol, en wat juist niet? We bespreken het hieronder.

✅ Do’s

1. **Zorg voor een duidelijk doel van de campagne.** Zorg dat je helder hebt wat het precieze doel is van de phishing-campagne. Wil je bewustzijn verbeteren en ervoor zorgen dat de medewerkers niet meer in phishingmails trappen of is het een nulmeting? Een duidelijk doel helpt bij het bepalen hoe je de phishing-campagne vormgeeft.

2. **Begin niet te moeilijk.** Start met enigszins eenvoudige en herkenbare scenario’s. Je kan de moeilijkheidsgraad gedurende het jaar verhogen. Zo voorkom je frustraties en verhoog je het bewustzijn op een geleidelijke manier.

3. **Koppel er directe feedback aan.** Laat medewerkers direct na klikken weten dat het een test was, met een korte uitleg of tips. Dat is hét leermoment. Bijvoorbeeld: “Deze e-mail was onderdeel van een training. Dit kan je herkennen aan de volgende punten: …”.

4. **Herhaling, herhaling en nog meer herhaling.** Beperk een phishing-test niet tot een eenmalige oefening maar voer deze meerdere keren uit per jaar. Om gedrag te kunnen veranderen is herhaling noodzakelijk.

5. **Communiceer transparant (op hoofdlijnen).** Laat medewerkers weten dat er in een bepaalde periode phishing-testen plaatsvinden. Niet exact wanneer of hoe, maar wel dát het gebeurt, en waarom. Zo houd je vertrouwen. Communiceer na afloop ook (op hoofdlijnen) de resultaten.

6. **Meet, leer en verbeter van de resultaten.** Analyseer wie klikte, wat werkte en waar de misverstanden zaten. Gebruik dit niet om te straffen, maar om gerichte training en extra uitleg aan te bieden.

🤦 Don’ts

1. **Niet ‘’namen en shamen’’.** Het doel van een phishing-campagne is bewustwording en gedragsverandering, niet afstraffen. Vermijd en individueel benoemen van de medewerkers die ‘’gefaald’’ hebben. Hierdoor kan je het vertrouwen van je medewerkers schaden.

2. **Vermijd gemene of gevoelige scenario’s.** Een nepbericht over ontslag, loonsverhoging of privéproblemen? Niet doen. Dat kan leiden tot klachten, boosheid of onveiligheid. Blijf ethisch verantwoord.

3. **Geen eenmalige oefening.** Eén campagne per jaar heeft weinig effect. Zet phishing-campagnes in als terugkerend onderdeel van een bredere security awareness-aanpak.

4. **Geen ‘’one size - fits all’’.** Zorg ervoor dat de phishingmails verschillend zijn per medewerkers. Zorg er daarnaast voor dat ze op verschillende momenten en tijdstippen verzonden worden. Zo weten de medewerkers niet van elkaar wanneer zij een phishingmail ontvangen en kunnen elkaar moeilijker op de hoogte brengen hiervan.

5. **Focus niet alleen maar op klikpercentages.** Bij het monitoren van de resultaten van een

De volledige versie van dit artikel vind u in de PRISM Kennisbank.

Contactgegevens
Audittrail
Sisalbaan 5a
2352 AZ Leiderdorp

071 - 747 71 71
bijpraten@audittrail.n