Tknika

Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre

SMARTFENSE:PHISHING

22-23 Ikasturtea (2.Kanpaina)

Fp EUSKADI LANBIDE HEZIKETA

EUSKO JAURLARITZA
GOBIERNO VASCO
HEZKUNTZA SAILA
Lanbide Heziketako Saiburuordetza
DEPARTAMENTO DE EDUCACIÓN
Viceconsejería de Formación Profesional

Aurkibidea

Aurkibidea

1.Helburuak-kokapena:

Phishing-a ziberdelitugileen **teknika gero eta ohikoagoa** da. Phishing-a zibergaizkileek erabiltzaileen informazio pertsonala eta finantzarioa lortzeko gehien erabiltzen duten teknika bihurtzen ari da, eta, ondorioz, kontzientziazio-kanpainak egin behar dira iruzurrezko praktika horietan ez erortzeko.

Arrazoi batzuk daude igoera honen nondik norakoak ulertzeko:

1. Teknologia eta **sare sozialen erabilera handiagoa:** Teknologiaren eta sare sozialen erabilera areagotzeak phishing erasoen eta bestelako iruzur zibernetikoen helburu izan daitezkeen pertsona gehiago ekarri ditu.
2. **Erabiltzaileen ezagutza** eta heziketa: Jende gehienak ez daki phishing zer den eta nola funtzionatzen duen; beraz, funtsezkoa da erabiltzaileak phishing arriskuez eta nola babes daitezkeen jabetzea.

   Kontzientziazio kanpainak egitea garrantzitsua da beraz, edozein antolakundetako datuen babeserako. Harimutur desberdinetan arreta jarri behar delarik:

1. Enpresa bateko langileentzako **sentsibilizazioa**: enpresak phishing-aren biktima izan daitezke, eta horrek datu konfidentzialak eta finantzarioak galtzea ekar dezake. Kontzientziazio-kanpainak egitea lagungarria izan daiteke langileak mehatxu mota horren inguruan sentsibilizatzeko eta eraso arrakastatsu baten arriskua murrizteko.
2. **Kostuen aurrezpena**: Kontzientziazio kanpainak inbertsio garrantzitsuak dira, baina epe luzerako kostuak aurrezten ere lagun dezakete, informazio baliotsua galtzea eta eraso zibernetiko garestiak saihesten baitituzte.

2.Kanpainaren iraupena:

Denboralizazioa:Maiatzak 2-16

- **Maiatzak 2:** Nola funtzionatzen du Phishing-ak? (Baliabidea:Momento Educativo-*Google segurtasun abixua*)
- **Maiatzak 3:** Phishing: honela lapurtzen dituzte zure datu pribatuak. (Baliabidea: Bideoa)
- **Maiatzak 4:** Phishing-a edo gure informazio pribatua egunero lapurtzeko modua. (Baliabidea: Newsletter)
- **Maiatzak 5:** Phishing: Posta elektroniko bidezko delitua (Baliabidea: Modulo interaktiboa)
- **Maiatzak 8:** Phishing: mehatxatzen gaituen arriskua. (Baliabidea:Momento Educativo - *LINKEDIN*)
- **Maiatzak 9:** Posta elektronikoa erabiltzearen arriskuak. (Baliabidea: Modulo interaktiboa)
- **Maiatzak 10:** Phishing: Posta elektroniko bidezko delitua. (Baliabidea: Azterketa)
- **Maiatzak 11:** Gupiren abenturak. (Baliabidea: Bideojokoa)
- **Maiatzak 12:** Nola hauteman dezakegu esteka arriskutsu bat? (Baliabidea:Momento Educativo-*Ransomwarea: UPS paketea jasotzeko*)
- **Maiatzak 15:** Ransomwarea: Gurea denaren truke ordaintzea. (Baliabidea: Modulo interaktiboa)
- **Maiatzak 16:** Interneteko helbide gaiztoak. (Baliabidea: Azterketa)

Hartzaileak: Tknikako langileak

3. Eduki bankua:

Smartfense-k kontzientziazio kanpaina burutzeko baliabide ezberdinak eskeintzen ditu. Hauen artean ezagunenak:

- **Modulu interaktiboak:**

Modulu interaktiboek gai ezberdinak aurkezten dituzte mota anitzeko jarduerak konbinatuz. Adibidez, multimedia eta GBL edukiak (Game-Based Learning). Horri esker, erabiltzaileak modu arin eta atseginean trebatzen joaten dira gai ugariren inguruan.

Erabili daitezkeen jarduera interaktibo batzuk hauek dira: Erantzun aukera anitzeko galderak ausazko ordenarekin, kontzeptuak arrastatzea eta askatzea, geziekin lotu, Phishing-eko mezu elektronikoak detektatu...

- **Bideoak:**

Bideoak, ikus-entzunezko edukiak diren heinean, erabiltzaileak kontzientziatzeko alternatiba dinamikoagoa dira.

Bideo bakoitzaren amaieran galderak gehitzeko aukera ematen dute, edukiak hobeto ulertze aldera.

- **Bideojokuak:**

Bideojokuak ere ikus-entzunezko edukiak diren heinean, Game Based Learning teknikenen bidez, zibersegurtasunean erabiltzaileak sentsibilizatu nahi ditu. Informazioaren segurtasuneko ohitura onei buruz jarduteko, modu atsegin eta dibertigarria da.

- **Newsletter:**

Newsletter-ak adituek diseinatutako e-mailak dira, etengabe eguneratzen direnak, eta erabiltzaileen arreta mantendu nahi dutenak jorratu beharreko hainbat gaitan. Newsletter bakoitzaren amaieran galderak gehitzeko aukera ematen da, irakurketa eta edukiak ulertzeko helburuarekin.

- **Phishing tresna:**

Phishing kanpainek, enpresen mezuak edo itxura baten komunikazio ofizial digital baten simulazioak, aukera ematen dute erabiltzaileek mota hortako mezuetan duten konfidantza maila neurtzeko. Konpainiaren edo langileen

informazio konfidentziala arriskuan jartzeko orduan dauden arrisku mailak neurtu daitezke modu honetan.

Phishing simulazio-kanpainetan, esleitutako erabiltzaileek jasoko duten phishing mezuan, aukera dute simulatutako webgune batetara estekatutako URLa ikusteko. Zentzu ohonetan, argitu behar da kanpaina guztiak SSL ziurtagiri baliodunak dituzten gune seguruetara zuzentzen direla.

- **Ransomware tresna:**

Ransomware-ko kanpainak, emailak bidaltzea, edo bestela, konpainiaren barne-komunikazioen bidalketak simulatzen dituzte. Erabiltzaileari, jasotako postatik edo esteka batetatik, fitxategi bat bere ordenagailuan deskargatzeko aukera ematen zaio.

Ekintza horietatik ateratako ondorioen bidez, sare administratzaileak jakingo du zenbat erabiltzaile amua irentsi duten eta bakoitzaren arrisku maila ebaluatu ahal izango du. Honela, enpresan aplikatu beharreko hobekuntza beharrak jakitearekin batera.

Ransomwareko simulazio-kanpainek ere, esleitutako erabiltzaileek jasoko duten URL baten aurrebista aurkezten dute simulazioan. Kasu honetan ere, SSL ziurtagiriak dituzten gune seguruetara zuzendutako kanpainak dira guztiak ere.

- **Momentu edukatiboak:**

Une edukatibo hauek, era labur eta eraginkorrean edukiak lantzeko modu bat dira. Hala nahi izanez gero, automatikoki Phishing edo Ransomware kanpaina baten barruan segurutzat jotzen ez den ekintza bat egitean aktibatzen dira.

- **Azterketak:**

Azterketak ezagutzak ebaluatzeko tresna tradizionalak dira. Ikaskuntza-prozesu oso baten, erabiltzaileen ezagutzak neurtzeko baliagarriak.

- **Inkestak:**

Inkestek, atal baten inguruko erabiltzaileen iritziak jasotzeko buruz balio dute, batez ere. Inkestek irudiak izan ditzakete, aukera anitzeko galderak, erantzun bakarra aukera daitezkenak, edo erantzun anitzak dituena, edota galdera irekiak, azken erabiltzaileari testua sartzera behartzen dituenak.

4. Emaitzak:

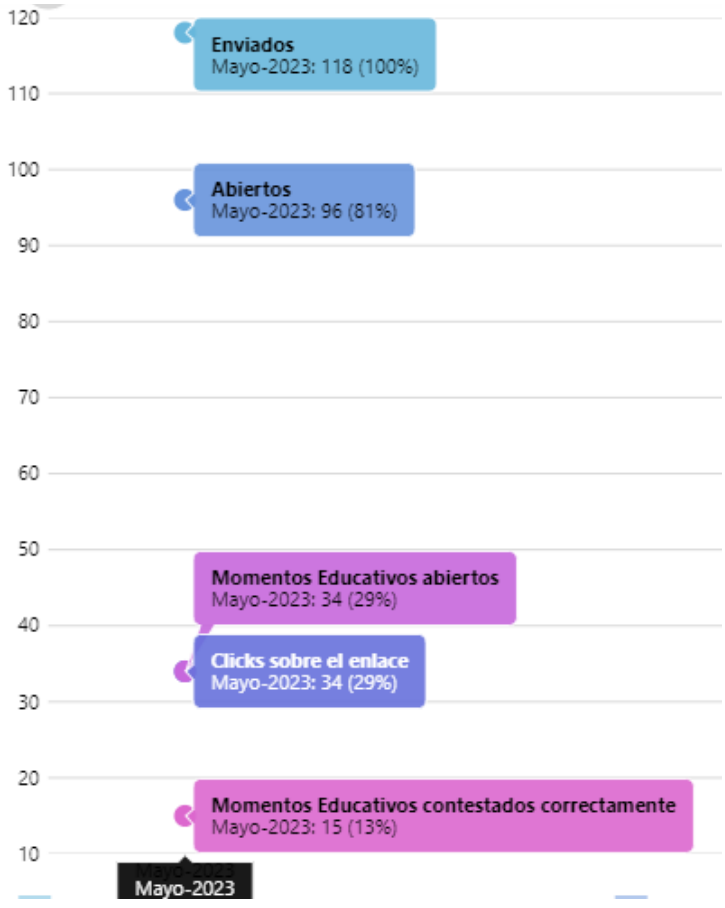
Kanpainaren helburu nagusia Phishing-aren eta Ransomware-aren inguruko kontzientziazioa sortzea izan denez, erabilitako baliabideak helburu horrekin sortuak izan dira.

Baliabide ezberdinak erabili diren arren, nagusiki Phishing eta Ransomware simulazioak izan dira ondorioak ateratzearen ikuspegitik, erreferentzia nagusienak.

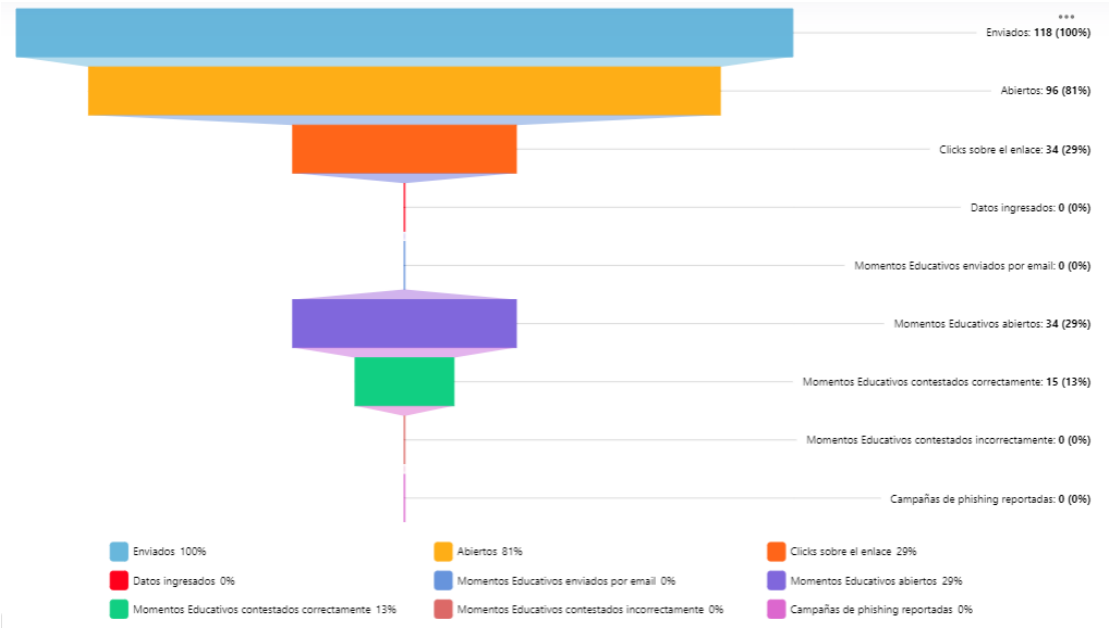
- **Phishing:**

Zentzu horretan, bi Phishing amu igorri dira email bidez bi data ezberdinetan, 118 bidalketa orotara. Lehendabiziko bidalketan "*Google segurtasun abixua*" simulatu da eta bigarrengoan aldiz, "*LINKEDIN profila ikusten ari dira*" simulazioa erabili da. Hauetatik, 96 mezu ireki dira, bidalitako mezuen %81 hain zuzen. Erantsita zeraman estekan berriz, 34 erabiltzailek klikatu dute (%29), arriskua dakarren ekintza modura ulertu daitekeena.

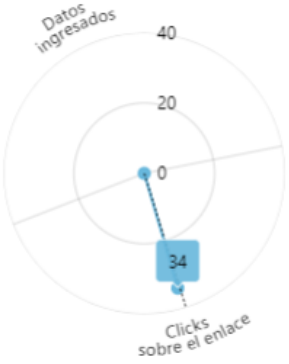
Estekaren gainean klikatzeak *"Momentu edukatiboak"* irekitzea aktibatzen zuenez, 34 erabiltzaile sartu dira berauek ikuskatzera, bukaeran erantzun beharreko galderei modu egokian 15 erabiltzailek erantzun dietelarik.



**Ikuspegi grafikoa:*



Irekitako mezuak:96

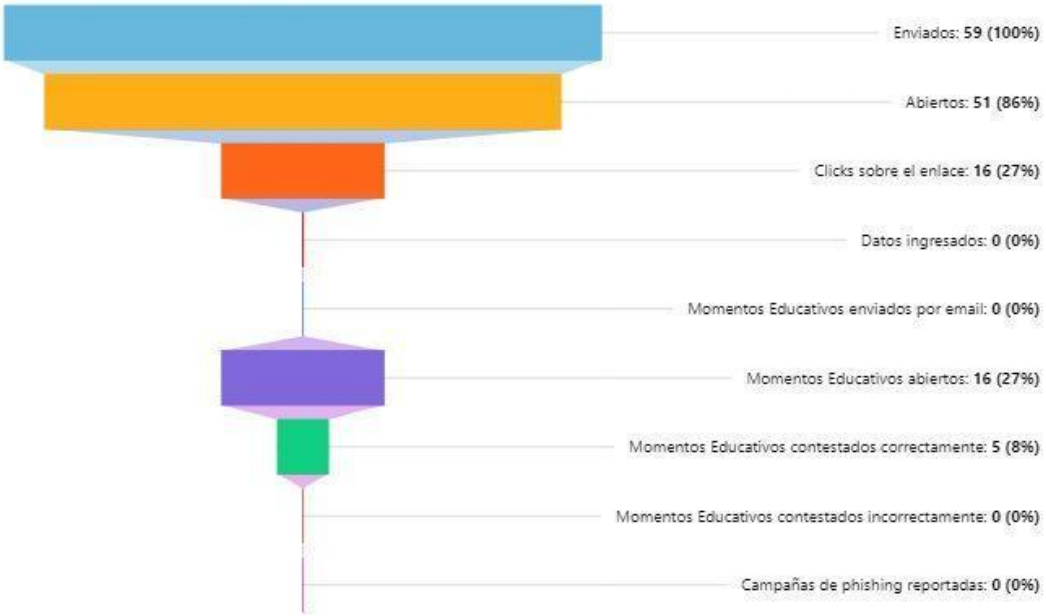


Estekan egindako klik kopurua:34

Esan modura, Phishing-ari loturiko bi bidalketa egin dira. Banan bana aztertu eta emaitzak konparatzen baditugu:

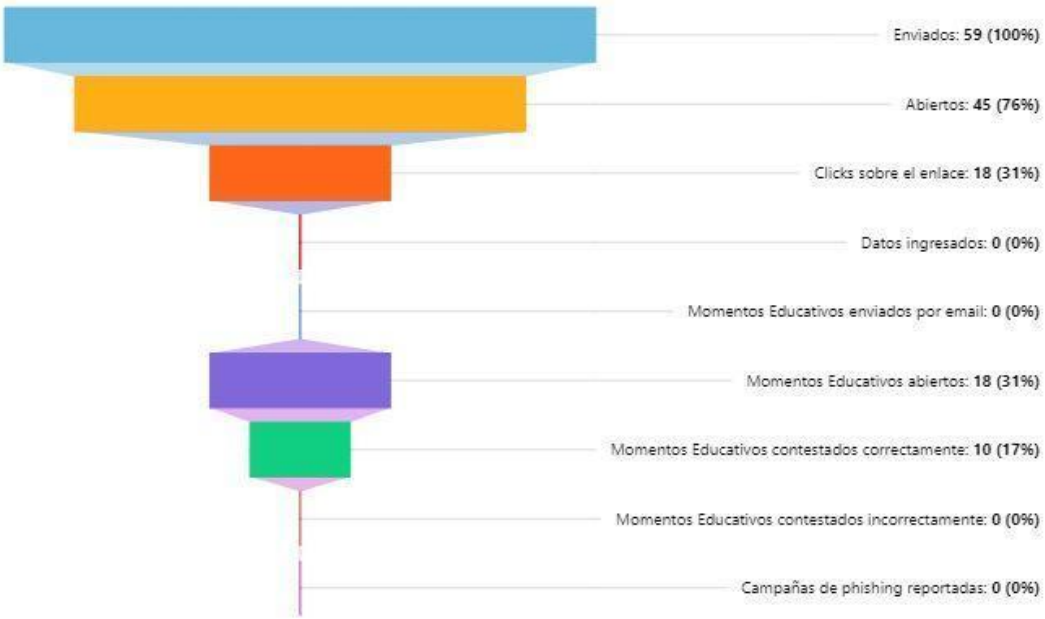
- **Phishing -1.bidalketa:** "*Google segurtasun abixua*"

59 erabiltzaileri bidali zaie mezua. Berauetatik 51 erabiltzailek ireki dute bidalitako emaila (%86), nahiz eta 16 erabiltzaile izan diren (%27) bidalitako link susmagarrian klikatu dutenak.



- **Phishing-2.bidalketa:** "*LINKEDIN profila ikusten ari dira*"

Kasu honetan, Linkedin profilari loturiko mezua igorri zaie 59 erabiltzaileri. Berauetatik 45ek ireki dute korreoa (%76) eta atxikita zeraman esteka susmagarrian 18 erabiltzailek (%31) egin dute klik.

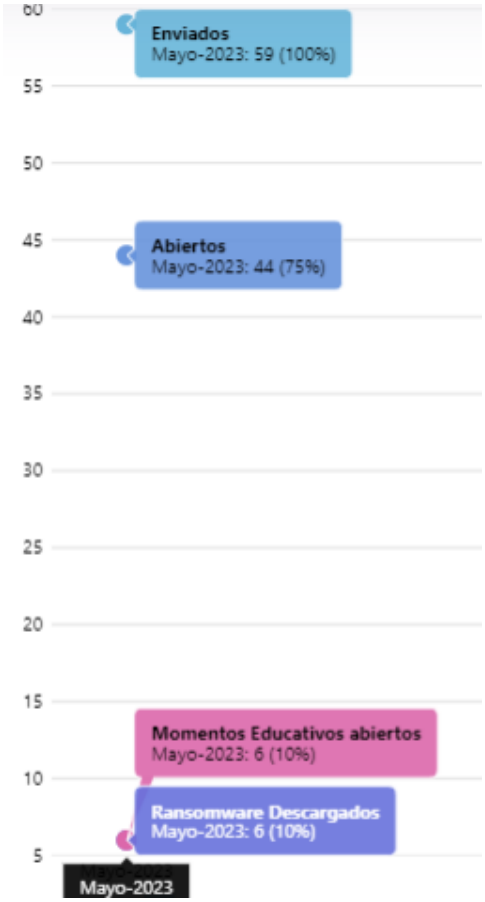


Bi bidalketen artean, antzeko emaitzak daudela ondorioztatu daiteke. Lehen bidalketa eta bigarrenaren arteko alderaketan, bai irekitze baita klikatze datu antzekoak daudelarik.

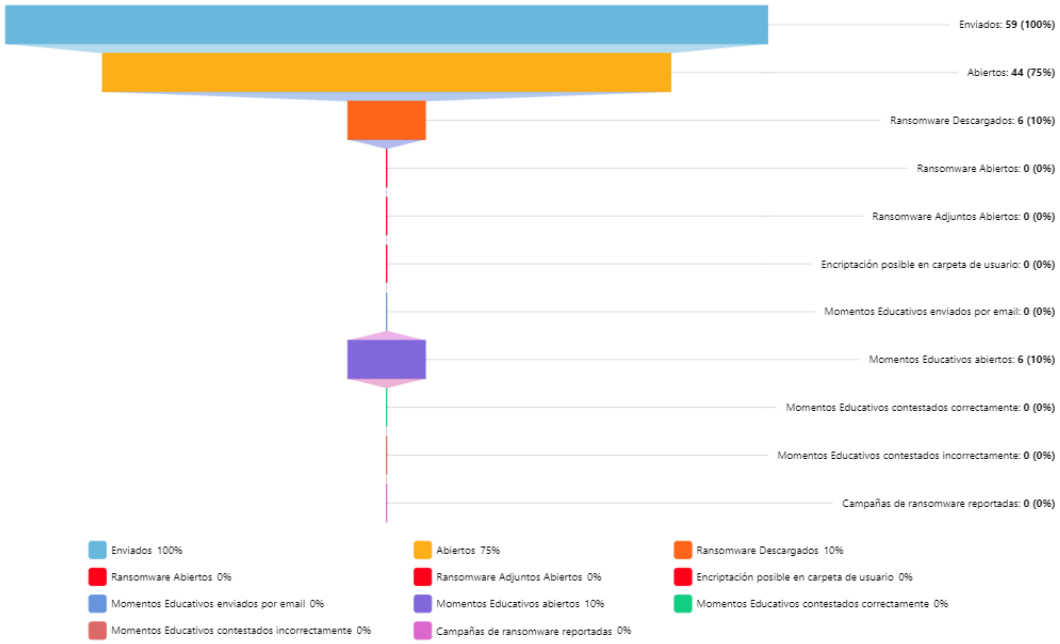
Mezuetan erantsitako esteketan klikatu duten erabiltzaileetan arreta jarri ezkero, bi bidalketetan klikatu duten zazpi erabiltzaile errepikatzen direla ikusi daiteke, gainontzekoak ezberdinak izan direlarik. Honi esker, arrisku taldeak lokalizatzeko aukera izango da, enpresako ahulguneak identifikatu eta berauetan, erabiltzaileen formakuntzan indar gehiago jartzeko.

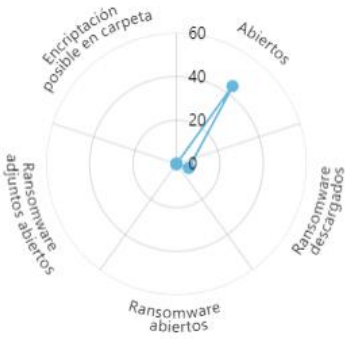
- **Ransomware:**

Phishing-arekin batera Ransomware itxurako amarruak testeatu dira. Berau egiteko, email bidezko bidalketa burutu da 59 erabiltzaileri zuzenduta. 59 erabiltzaile hauetatik 44 erabiltzailek ireki dute korreoa, bidalitakoen %75.
Ireki duten erabiltzaile hauetatik, 6 pertsonak deskargatu dute ransomwarea, bidalitakoen artetik %10 gutxigorabehera. Hauen artetik, 4 erabiltzaile izan dira, aurreko Phishing bidalketaren batetan estekan klikatu dutenak. 6 pertsona hauetako inork, ez du erantzun ransomwarea deskargatzean irekitzen zitzaien *"Momentu edukatiboa"*.



**Ikuspegi grafikoa:*



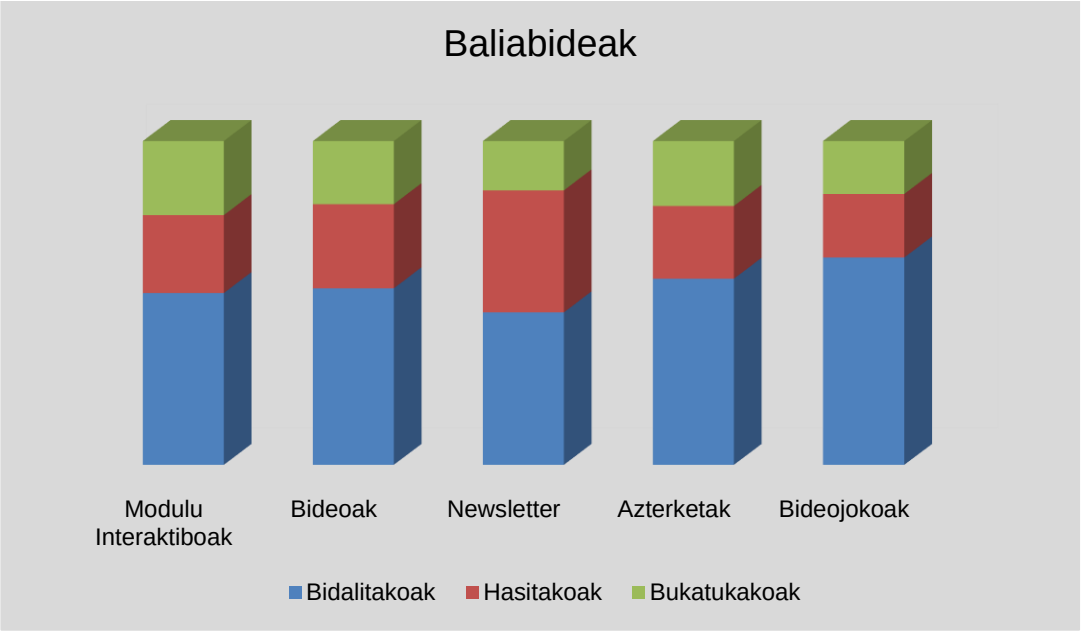


Irekitako mezuak:59

Deskargatutako ransomwarea:6

Kontzientziazio kanpaina honetan, **Phishing** eta **Ransomware** bidalketekin batera, eduki ezberdinak jorratu dira erabiltzailei formakuntza eman nahirik. Jorratu diren **edukien** artean:

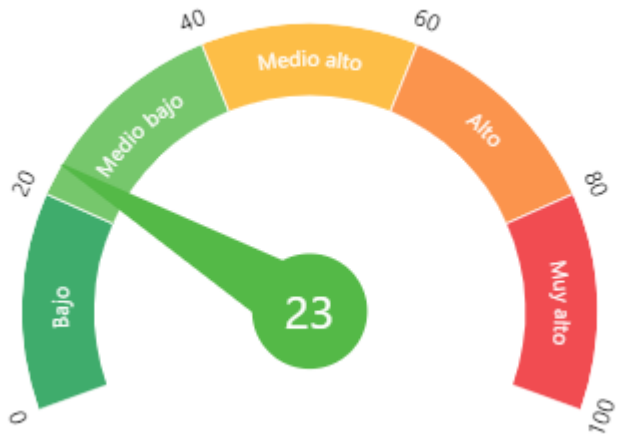
BALIABIDE MOTA	BIDALKETA KOPURUA	BIDALITAKOAK	HASITAKOAK	BUKATUTAKOAK
Modulu Interaktiboak	**3**	**177**	**80**(%45)	**76**(%43)
Bideoak	**1**	**59**	**28** (%47)	**21**(%36)
Newsletter	**1**	**59**	**47** (%80)	**19**(%32)
Azterketak	**2**	**118**	**46**(%39)	**41**(%35)
Bideojokoak	**1**	**59**	**18**(%31)	**15**(%25)



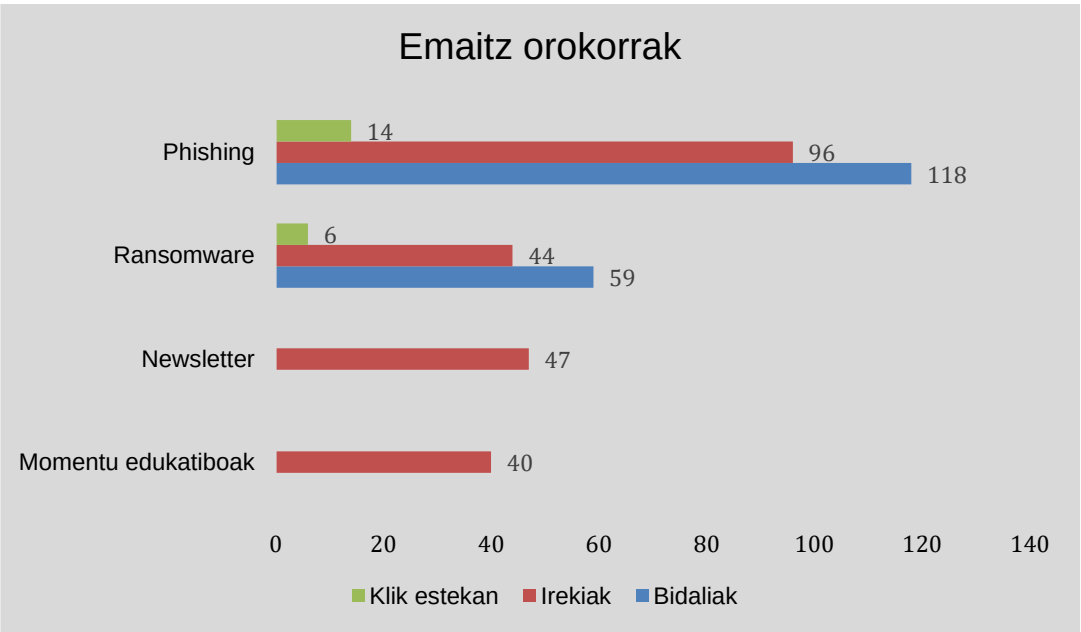
5.Ondorioak:

Esan bezala, Smartfense tresnak eskeintzen dituen euskarri ezberdinak erabiliz burutu den kontzientziazio kanpaina honetan, Phishing eraso bat jasotzeko Tknikak antolakunde modura dituen arrisku mailak neurtu nahi izan dira.

Burutu diren simulazioetan ikusitakoagatik, bertako langileak lan ohitura onak dituztela orokorrean ondorioztatu dezakegu. Smartfensek erabiltzen duen **100eko arrisku indize batetik 23ko arrisku maila** lortu delarik. Neurgailu honen arabera, Tknikaren arrisku maila, **MEDIO BAJO** modura kalifikatu daitekelarik.



Emaitzak hauek izanik ere, antolakundean egon daitezken hutsuneak detektatu eta aurrerantzean hauen hobekuntzan egin beharreko inbertsioen inguruan hausnartzea komeni da.



Ondorio modura, aukeran dauden errekurtsoak zaintza teknologikoan inbertitzea komenigarria izango da aurrerantzean ere. Ikuspegi teknikoan, email zerbitzuan mezu susmagarriak iragaztearen ikuspegitik, edota sistemak eguneratuta izatearen beharrera. Baita giza ikuspegian ere, kontzientziazioan eta sarean dauden mehatxuen inguruan lanketa eginez, eta langileen artean formakuntzan sakonduz.

Etorkizunean ere mehatxu berriak izango dira ate joka, eta zentzu honetan, etengabeko hobekuntzaren ikuspegitik, adi jarraitu beharko dira saretik datozen arrisku berriak.