Tknika

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

GOPHISH

2023

Fp EUSKADI LANBIDE HEZIKETA

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

AURKIBIDEA

1. SARRERA

Phishing-a, erasotzaileak biktimak engainatuz, informazio konfidentziala eskuratzeko eraso zibernetiko mota bat da. Beronen bidez, pasahitzak, kreditu-txartelen zenbakiak edo identifikazio pertsonaleko datuak lortzen ahalegintzen dira. Phishing-erasoak mezu elektronikoen edo testu-mezuen bidez egiten dira, eta hasiera baten iturri fidagarrietakoak direla dirudien arren, atzean amarru bat izaten dute normalean.

Gophish kode irekiko phishing tresna bat da, erabiltzaileei phishing posta elektroniko pertsonalizatuak sortu eta bidaltzeko aukera ematen diena. Tresna erabilerraza da, eta zibersegurtasunean edozein esperientzia duten pertsonek erabil dezakete. Doakoa da eta kode irekikoa.

Dokumentu honetan, phishing eraso bat nola simulatu azaltzen da, burutu beharreko instalazioa eta **Gophish** produktuari buruzko informazioa azalduz. Landu hurrengo gaiak:

- Erasoa garatuko den ingurunea
- Gophish instalazioa
- Gophish konfigurazioa
- Erasoaren simulazioa
- Nola babestu phishing-etik

Dokumentu honen helburua phishing-aren oinarrizko ulermena emateaz gain, **Gophish** bidez segurtasunari buruzko sartze eta kontzientziazio-probak egiteko erabilera azaltzea da.

2. Domeinua eta Prestaketa

Eraso-simulazioa **Hezigunea**-ko webgunea simulatuz egitea planteatu denez, lehendabizi beronen antzekoa den domeinu bat erosi da. Bilaketa bat egin ondoren, **hezigunea.net** helbidea erosi eta berau **Cloudflare** bidez konfiguratu da.

3. Erasoaren Ingurunea

Phishing erasoaren simulakroa, ingurune erreal baten egin nahi izan denez, barne saretik kanpora ere erasoak eragina izateko helburuarekin, GOPHISH instalatzeko zerbitzaria kanpoko ingurune batetan instalatu dugu. AWS, Contabo…edo honelako zerbitzuren batek balioko luke ezaugarri hauetako eraso bat gauzatzeko.

Kasu honetan, **AWS-n** altxatutako **EC2 LINUX** bat jarri da produkzioan (44.196.151.67 IP elastikoarekin) **Debian** makina batetan montatu delarik **GOPHISH** instalatu den azpiegitura. Plataformak berak esleitutako IP publikoa izan delarik ondorengo zereginetan erabilitako helbidea.

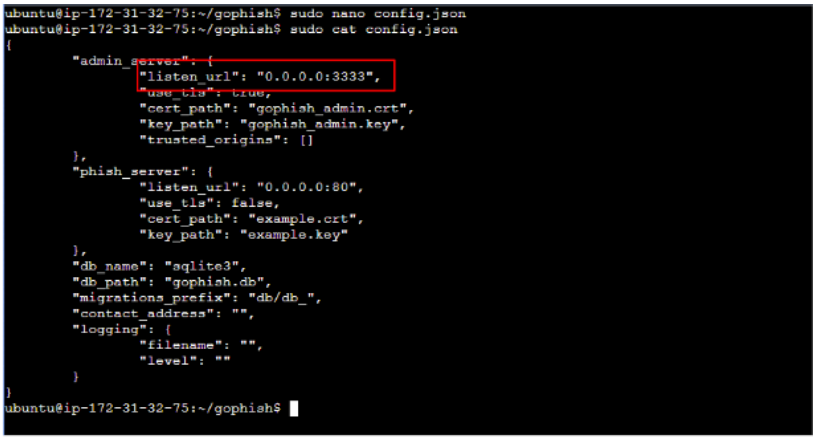
- Makinari ezarri zaizkion baliabideak:
    - CPU: 2
    - RAM: 8GB
    - SSD: 25 GB
    - Sareak:IP publikoa
    - Irekitako portuak:
        i. 80
        ii. 443
        iii. 22
        iv. 3333—kudeaketa portua

4. Gophish: deskarga eta instalazioa

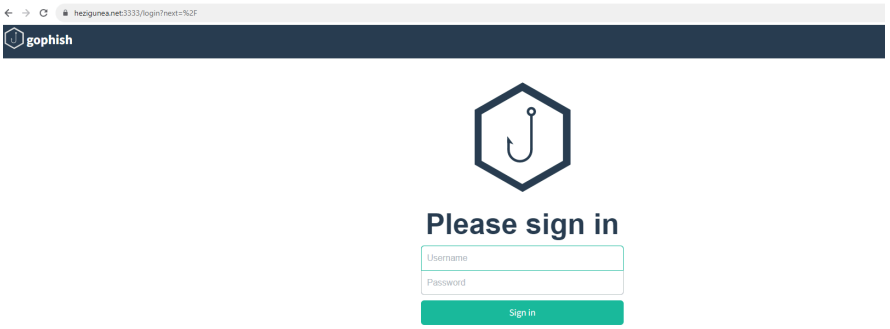
EC2 ko zerbitzarira SSH bidez logeatu eta **GOPHISH** deskargatu eta instalatzea izango da hurrengo urratsa. Nola egin azalduz, hona hemen informazio gehiago https://getgophish.com/documentation/

a. Deskargatu: https://github.com/gophish/gophish/releases

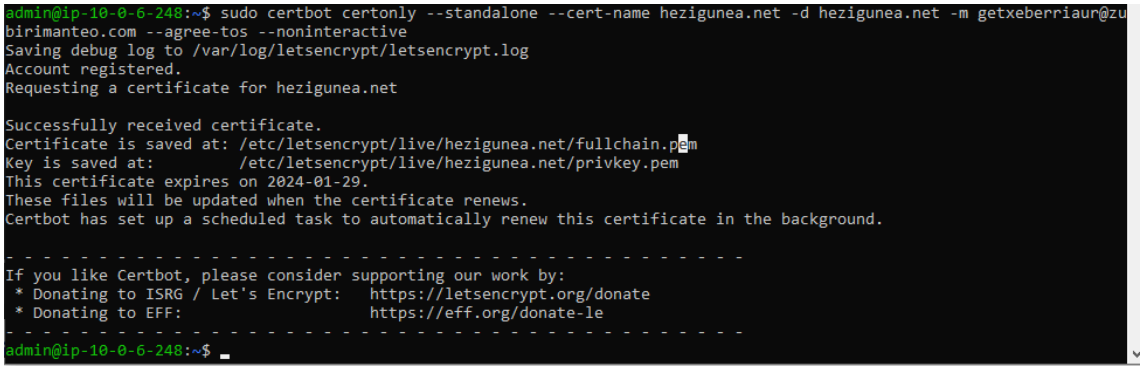
b. Makinan **gophish** izeneko karpeta bat sortu eta bertan deskonprimitu.
c. IP helbidea aldatu: **config.json** fitxategian. Kanpoko makina batetatik konektatu ahal izateko **0.0.0.0:3333** utzita nahikoa da.



d. Gophish arrankatu ondoren, nabigatzailean gure zerbitzariaren IP helbidea jarri eta **3333 portutik** kudeatu ahal izango dugu aurrerantzean GOPHISH.



e. Hau eginik, webguneen **zertifikazioekin** arazorik ez izateko, eta erabiliko diren webguneak fidagarriak direla irudikatzeko, auto-sinatutako zertifikatuak instalatu behar dira zerbitzarian eta **443** portutik ezarri aterabidea.

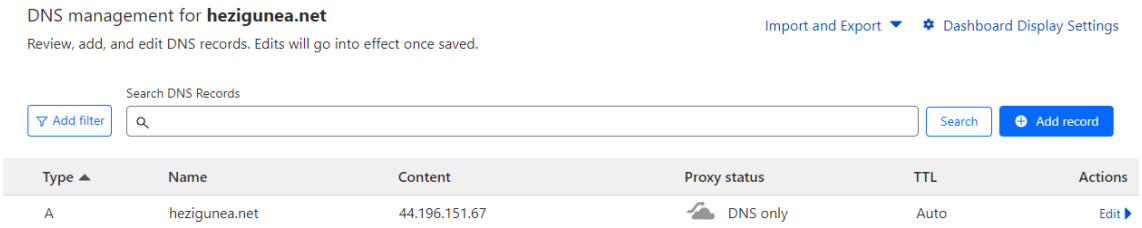


Certificate is saved at: */etc/letsencrypt/live/hezigunea.net/fullchain.pem*
Key is saved at: */etc/letsencrypt/live/hezigunea.net/privkey.pem*

i. Lehen egin modura, **config.json** aldatu:
ii. Giltzak erantsi eta **443** portua jarri eta **use_tls:t**rue

SSH bidez konektatzen denez, **GOPHISH** arrankatuta geratu dadin, **./gophish** bigarren planoan exekutatzeko eta SSH sesioa ixtean funtzionatzen jarraitzeko: **nohup sudo ./gophish &** agindu bidez exekutatzea komeni da.

Cloudflare-n gure **DNS**-a, **GOPHISH** instalatuta dugun EC2 instantziaren IP helbidera begira jartzea ere ezinbestekoa da.



5. POSTA ZERBITZARIA KONFIGURATU

CONTABO plataforman beste zerbitzari bat kokatu da posta zerbitzaria bertan instalatzeko. Zerbitzua martxan jartzeko dauden aukeren artean, aukera bat **Poste.io** instalatzea da Docker bidez eta beronen azpiegitura erabiltzea posta helbide guztiak sortzeko. Gida hau jarraitu dugu:

https://hailbytes.com/how-to-set-up-a-working-smtp-email-server-for-phish-testing/

Docker instalatu dugu bertan.
Poste.io repositorioa deskargatu eta posta zerbitzaria arrankatu. Bertan, **mail.hezigunea.net** posta zerbitzua martxan jarri container batetan.

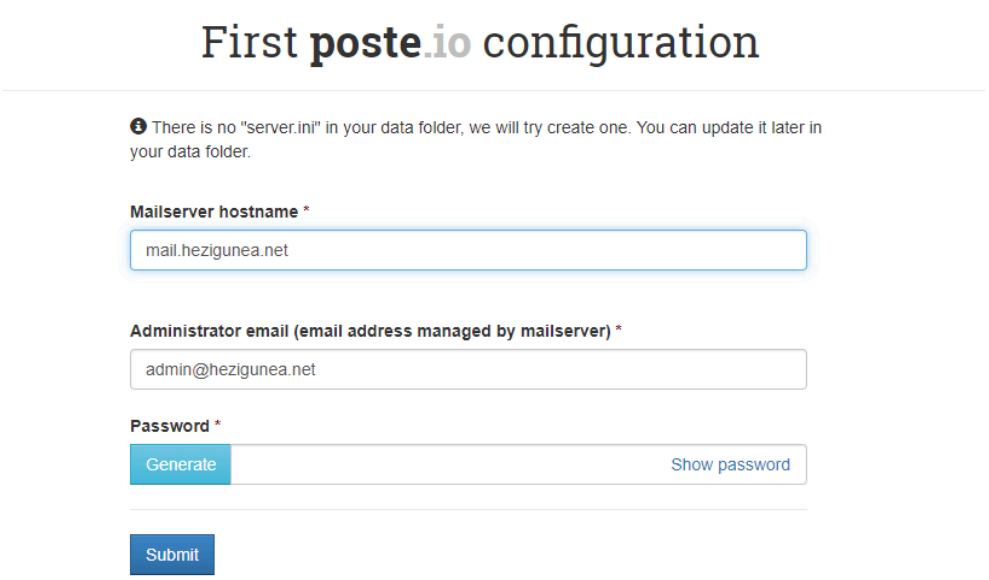
```
$ docker run \
    --net=host \
    -e TZ=Europe/Prague \
    -v /home/data:/data \
    --name "mailserver" \
    -h "mail.hezigunea.net" \
    -t analogic/poste.io
```

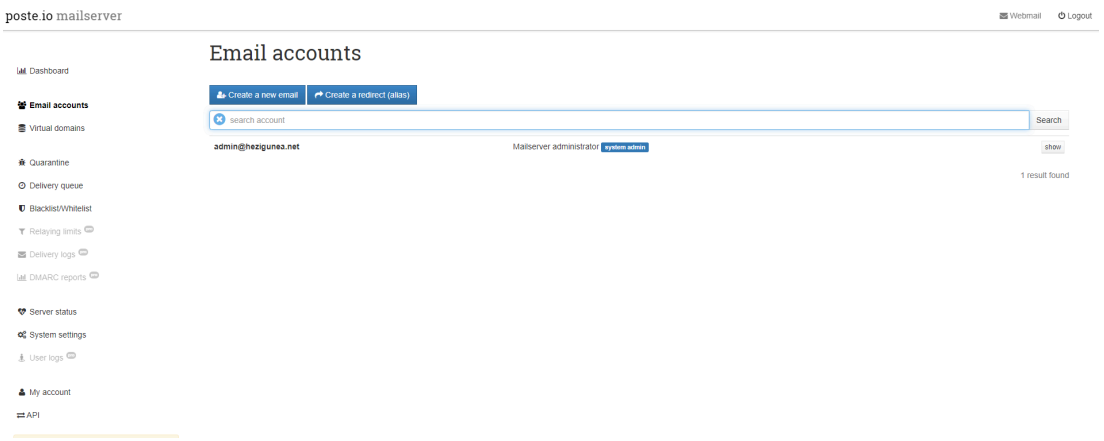

Tknika
Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre

```
root@vmi1508494:~# docker ps -a
CONTAINER ID   IMAGE              COMMAND    CREATED          STATUS                      PORTS     NAMES
fb948fba656d   hello-world        "/hello"   11 minutes ago   Exited (0) 11 minutes ago             modest_dubinsky
94f17a8f3f01   analogic/poste.io  "/init"    3 hours ago      Exited (0) 45 minutes ago             mailserver
8ee6fbd7ccb7   hello-world        "/hello"   4 hours ago      Exited (0) 4 hours ago                confident_williams
```

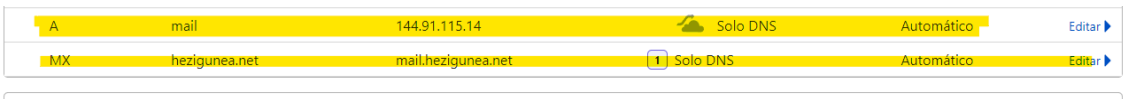
Contaboko zerbitzariaren IP helbidea jarriz, administrazio panelean sartu eta emailak sortu.

admin@hezigunea.net
no-reply@hezigunea.net





Cloudflaren DNS atalean gehitu posta zerbitzariaren datuak:



MEZUAK AUTENTIKATU:

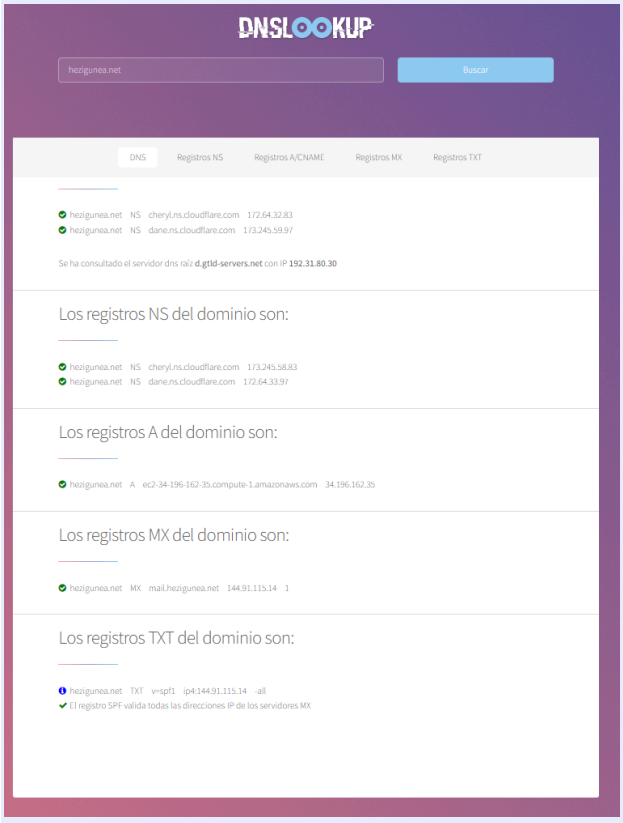
Posta zerbitzariaren bidez sorturiko kontuak fidagarriak izan daitezen, antispam politiken aurrean, eremu desberdinak konfiguratzea aholkatzen da. **PF,DKIM,DMARC**

- **SPF**: Antispam filtroa
  INFORMAZIO iturria:http://www.open-spf.org/SPF_Record_Syntax/

Domeinuko erregistroetan TXT sarrera bat gehitu dugu eta bertan, SPF baliozkotze bat erantsi da korreo zerbitzariko Iparekin.

```
v=spf1 ip4:144.91.115.14 -all
```

DNSLOOKUP (dnslookup.es) webgunean erabiliko den domeinuaren bilaketa bat egin eta SPF iturri fidagarriak dituela ikusi.



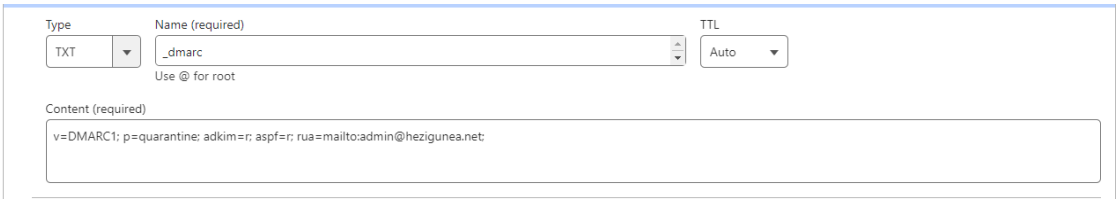
- **DKIM** erregistroa:

Poste.io-n DKIM giltza berri bat sortzeko eskatu eta ondoren, berau Cloudflareko portaleko TXT motako sarrera modura itsatsi. Honelako antzeko egitura duen karaktere kate bat izango litzateke:

```
s20231109283._domainkey.hezigunea.net. IN TXT "k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvk6WrsBWbL3retoBCZ137S1R6P9z2Hf2
HE96MXGVq8UG5I7zhxtIiumGIUmy9oa/dvOXSK+PP9znET/1L7X7ZQSuK3hWZ6D11/tTeovXjfh30g
TflRLhDNw+V4COxT+MPuGYt21aueZ2dEg9tiapV29eDhiCD2nJGJMdAKatEtseN9Y7cN1fC8X6+u8Z
OnM1kB+xCP1QQivAuH3SB6eQffh17tzhUz5E56I8RFQzgmjhc1MwOtVVXHbJSMws3n3u1vV2ZxAqaP
rfuuUxabw5bmW6hsCruDquWZiUSe/OhW+zn11dpf6iu1Pfv9Tv3TX8LniqsNpEPPc4DlLSCwO62QID
AQAB"
```

- **DMARC**:

SPF eta DKIM iragazkiak ez badira gainditzen, mezuak kuarentenan utzi eta mezu bat bidaltzeko nahi den korreora.

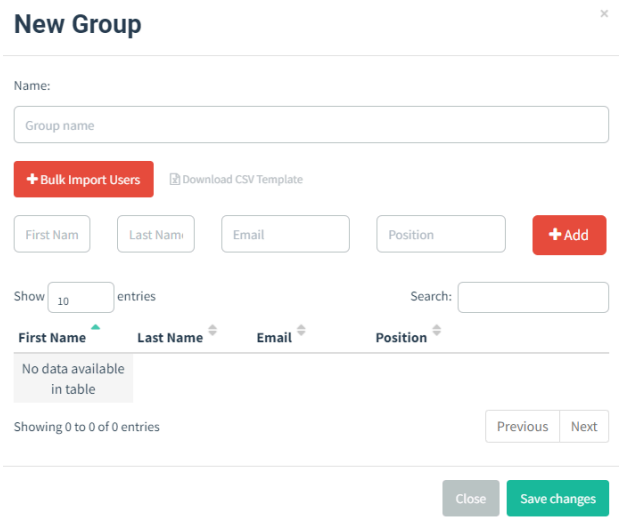


Modu honetara gelditu dira **Cloudflareko DNS** erregistroak:

Type	Name	Content	Proxy status	TTL	Actions
A	hezigunea.net	44.196.151.67	DNS only	Auto	Edit
A	mail	144.91.115.14	DNS only	Auto	Edit
CNAME	mentimeter	hezigunea.net	DNS only	Auto	Edit
MX	hezigunea.net	mail.hezigunea.net	1 DNS only	Auto	Edit
PTR	mail	35.162.196.34.in-addr.arpa	DNS only	Auto	Edit
TXT	_dmarc	v=DMARC1; p=quarantine; adkim=r; aspf...	DNS only	Auto	Edit
TXT	hezigunea.net	google-site-verification=_RCMlwgS7WyfL...	DNS only	Auto	Edit
TXT	hezigunea.net	v=spf1 ip4:144.91.115.14 -all	DNS only	Auto	Edit
TXT	s20231121165._domainkey	v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w...	DNS only	Auto	Edit

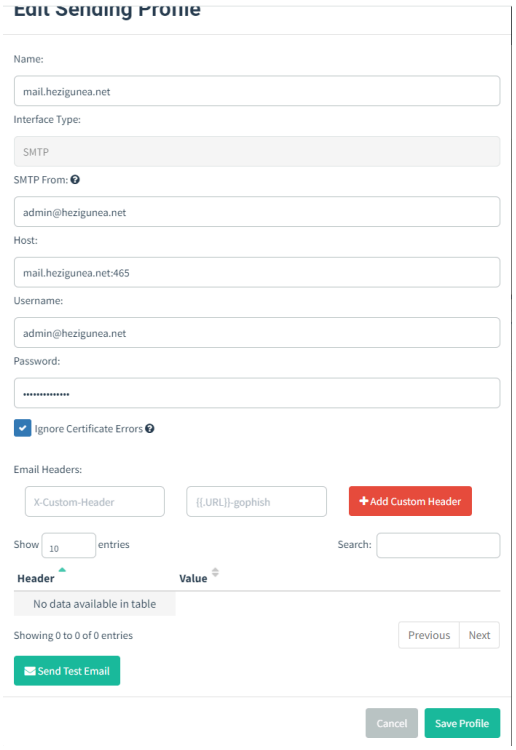
6. GOPHISH KONFIGURATZEN

- **Erabiltzaileak** sortu eta taldekatu.

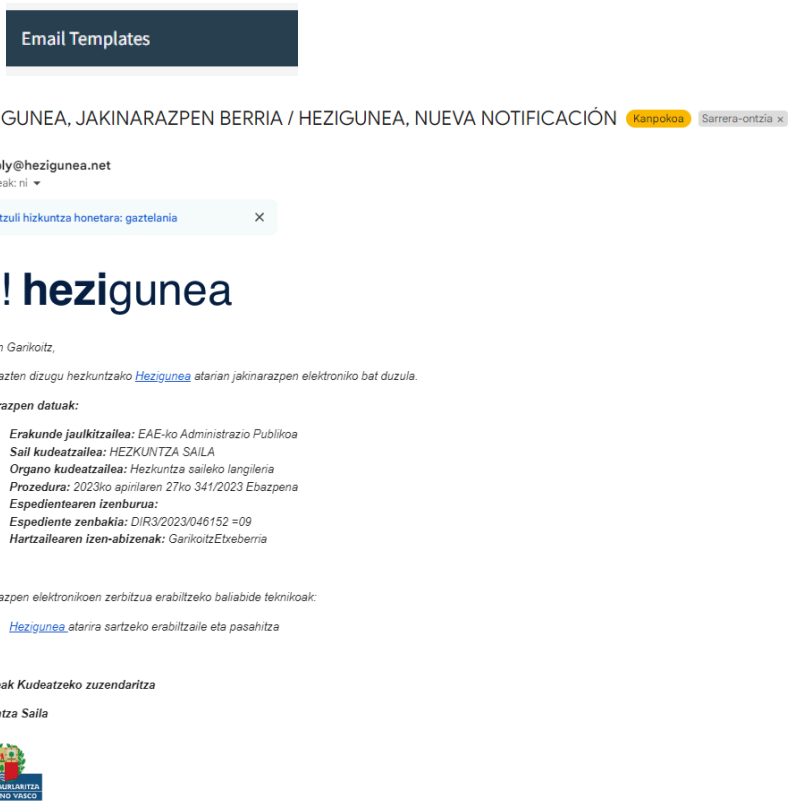


- **SMTP** zerbitzaria konfiguratu.

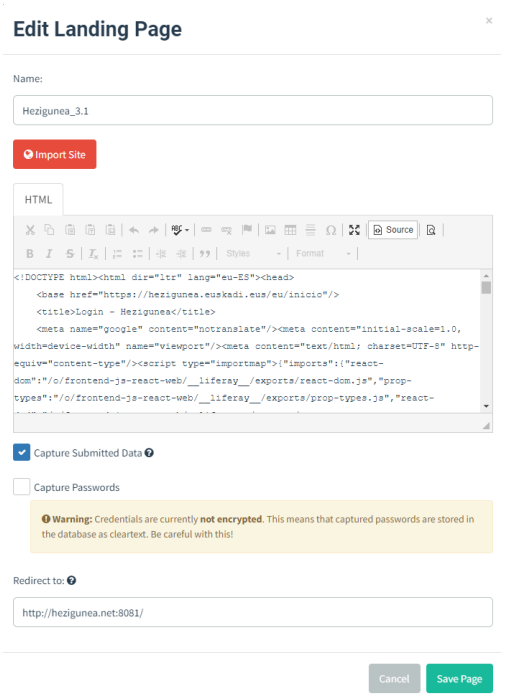
Tknika
Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre



- **Email txantiloi** bat prestatu (gure kasuan Heziguneako irudi eta itxurarekin):



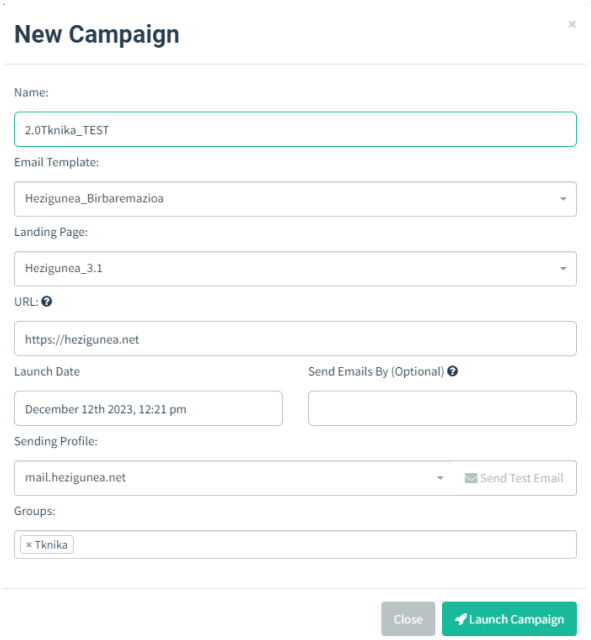
- **Landing page** bat osatu. Ordezkatu nahi den webgunea simulatu. Inportatu txantiloia



Kredentzialak sartzen dituzten erabiltzaileak phishing kanpaña baten biktima izan direla azalduz beste helbide batetara bideratuko dira. Egokiena **ohartarazpena** azaltzen den **webgune** batetara bideratzea izango litzateke.

- **KANPAINAK abiarazi** eta bidalketak programatu:
    - Hautatu **smtp** zerbitzaria

- Hautatu **email** txantiloia.
- Hautatu birbidali beharreko **webgunearen** helbidea (Landing page domeinua)
- **Groups** atalean zein talderi zuzenduta dagoen adierazi.



7. BIBLIOGRAFIA:

- https://getgophish.com/documentation/
- https://www.techrepublic.com/article/how-to-run-a-phishing-attack-simulation-with-gophish/
- https://www.golinuxcloud.com/create-phishing-campaign-gophish/
- https://redfoxsec.com/blog/phishing-simulations-with-gophish/
- https://poste.io/doc/configuring-dns

Tknika

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

Zamalbide Auzoa z/g - 20100 Errenteria (Gipuzkoa) - T. (+34) 943 082 900 - info@tknika.eus –
www.tknika.eus