



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

# GOPHISH

## 2023



## AURKIBIDEA

<b>1. SARRERA.....</b>	<b>1</b>
<b>2. Domeinua eta Prestaketa.....</b>	<b>2</b>
<b>3. Erasoaren Ingurunea.....</b>	<b>2</b>
<b>4. Gophish: deskarga eta instalazioa.....</b>	<b>2</b>
<b>5. Posta zerbitzaria konfiguratu.....</b>	<b>4</b>
<b>6. Gophish Konfiguratzeko.....</b>	<b>7</b>
<b>7. Bibliografia:.....</b>	<b>10</b>

# 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 elektronikoa pertsonalizatuak sortu eta bidaltzeko aukera ematen diena. Tresna erabilerraza da, eta zibersegurtasunean edozein esperientzia duten pertsonak 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
- Erasoren simulazioa
- Nola babestu phishing-etik

Dokumentu honen helburua phishing-aren oinarritzko 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

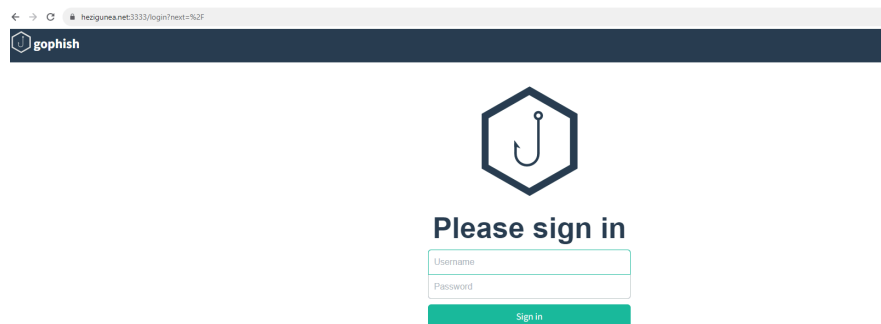
**EC2** ko zerbitzarira SSH bidez logeatu eta **GOPHISH** deskargatu eta instalatzea izango da hurrengo urratsa. Nola egin azalduz, hona hemen informazio gehiago <https://getgophish.com/documentation/>

- a. Deskargatu: <https://github.com/gophish/gophish/releases>

- b. Makin **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.

```
ubuntu@ip-172-31-32-75:~/gophish$ sudo nano config.json
ubuntu@ip-172-31-32-75:~/gophish$ sudo cat config.json
{
  "admin_server": {
    "listen_url": "0.0.0.0:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key",
    "trusted_origins": []
  },
  "phish_server": {
    "listen_url": "0.0.0.0:80",
    "use_tls": false,
    "cert_path": "example.crt",
    "key_path": "example.key"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": "",
  "logging": {
    "filename": "",
    "level": ""
  }
}
```

- 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.

```
admin@ip-10-0-6-248:~$ sudo certbot certonly --standalone --cert-name hezigunea.net -d hezigunea.net -m getxerberriaun@zu
birimanteo.com --agree-tos --noninteractive
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Account registered.
Requesting a certificate for hezigunea.net
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/hezigunea.net/fullchain.pem
Key is saved at: /etc/letsencrypt/live/hezigunea.net/privkey.pem
This certificate expires on 2024-01-29.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

-----
If you like Certbot, please consider supporting our work by:
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
* Donating to EFF: https://eff.org/donate-le
-----
admin@ip-10-0-6-248:~$
```

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:true**

```
admin@ip-10-0-6-248: ~/gophish
GNU nano 7.2 config.json

{
  "admin_server": {
    "listen_url": "0.0.0.0:3333",
    "use_tls": true,
    "cert_path": "/etc/letsencrypt/live/hezigunea.net/fullchain.pem",
    "key_path": "/etc/letsencrypt/live/hezigunea.net/privkey.pem",
    "trusted_origins": []
  },
  "phish_server": {
    "listen_url": "0.0.0.0:443",
    "use_tls": true,
    "cert_path": "/etc/letsencrypt/live/hezigunea.net/fullchain.pem",
    "key_path": "/etc/letsencrypt/live/hezigunea.net/privkey.pem"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": "",
  "logging": {
    "filename": "",
    "level": ""
  }
}
```

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.

DNS management for **hezigunea.net** Import and Export Dashboard Display Settings

Review, add, and edit DNS records. Edits will go into effect once saved.

Search DNS Records

▼ Add filter  Search + Add record

Type ▲	Name	Content	Proxy status	TTL	Actions
A	hezigunea.net	44.196.151.67	DNS only	Auto	<a href="#">Edit</a>

## 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 repositoria 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
```

```

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 jarritz, administrazio panelean sartu eta emailak sortu.

[admin@hezigunea.net](mailto:admin@hezigunea.net)  
[no-reply@hezigunea.net](mailto:no-reply@hezigunea.net)

## First poste.io configuration

There is no "server.ini" in your data folder, we will try create one. You can update it later in your data folder.

**Mailserver hostname \***

mail.hezigunea.net

**Administrator email (email address managed by mailserver) \***

admin@hezigunea.net

**Password \***

Generate

Show password

Submit

poste.io mailserver Webmail Logout

**Email accounts**

Create a new email Create a redirect (alias)

Search account

admin@hezigunea.net Mailserver administrator system admin

show

1 result found

- Dashboard
- Email accounts
- Virtual domains
- Quarantine
- Delivery queue
- Blacklist/Whitelist
- Relaying limits
- Delivery logs
- DMARC reports
- Server status
- System settings
- User logs
- My account
- API

Cloudflaren DNS atalean gehitu posta zerbitzariaren datuak:

A	mail	144.91.115.14	Solo DNS	Automático	Editar
MX	hezigunea.net	mail.hezigunea.net	Solo DNS	Automático	Editar

## MEZUAK AUTENTIKATU:

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

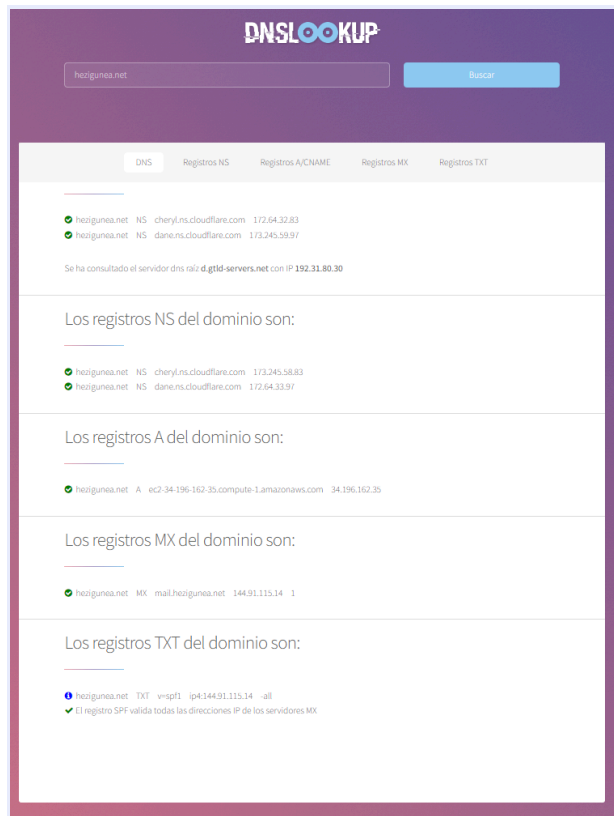
- **SPF:** Antispam filtroa

INFORMAZIO iturria: [http://www.open-spf.org/SPF\\_Record\\_Syntax/](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=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvk6WrsBWbL3retoBCZ137S1R6P9z2Hf2HE96MXGVq8UG5I7zhxtIiumGIUmy9oa/dvOXSK+PP9znET/1L7X7ZQSuK3hWZ6D11/tTeovXjfh30gTf1RLhDNw+V4COxT+MPuGYt21aueZ2dEg9tiapV29eDhiCD2nJGJMDAKatEtseN9Y7cN1fC8X6+u8ZOnM1kB+xCP1QQivAuH3SB6eQffh17tzhUz5E56I8RFQzgmjhc1MwOtVVXHbJSMws3n3u1vV2ZxAqaPrfuuUxabw5bmW6hsCruDquWZiUse/OhW+zn11dpf6iu1Pfv9Tv3TX8LniqsNpEPPc4D1LSCwO62QIDAQAB"`

- **DMARC:**

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



Type: TXT Name (required): \_dmarc TTL: Auto

Use @ for root

Content (required): v=DMARC1; p=quarantine; adkim=r; aspf=r; rua=mailto:admin@hezigunea.net;

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

Type ▲	Name	Content	Proxy status	TTL	Actions
A	hezigunea.net	44.196.151.67	DNS only	Auto	<a href="#">Edit ▶</a>
A	mail	144.91.115.14	DNS only	Auto	<a href="#">Edit ▶</a>
CNAME	mentimeter	hezigunea.net	DNS only	Auto	<a href="#">Edit ▶</a>
MX	hezigunea.net	mail.hezigunea.net	DNS only	Auto	<a href="#">Edit ▶</a>
PTR	mail	35.162.196.34.in-addr.arpa	DNS only	Auto	<a href="#">Edit ▶</a>
TXT	_dmarc	v=DMARC1; p=quarantine; adkim=r; aspf=r; rua=mailto:admin@hezigunea.net;	DNS only	Auto	<a href="#">Edit ▶</a>
TXT	hezigunea.net	google-site-verification=_RCMIwgS7Wyl...	DNS only	Auto	<a href="#">Edit ▶</a>
TXT	hezigunea.net	v=spf1 ip4:144.91.115.14 -all	DNS only	Auto	<a href="#">Edit ▶</a>
TXT	s20231121165_domainkey	v=DKIM1; k=rsa; p=MIIlBjANBgkqhkiG9w...	DNS only	Auto	<a href="#">Edit ▶</a>

## 6. GOPHISH KONFIGURATZEN

- **Erabiltzaileak** sortu eta taldekatu.

**New Group** ×

Name:

[+ Bulk Import Users](#) [Download CSV Template](#)

[+ Add](#)

Show  entries Search:

**First Name** **Last Name** **Email** **Position**

No data available in table

Showing 0 to 0 of 0 entries [Previous](#) [Next](#)

[Close](#) [Save changes](#)

- **SMTP** zerbitzaria konfiguratu.

### Edit Sending Profile

Name:

Interface Type:

SMTP From:

Host:

Username:

Password:

☒ Ignore Certificate Errors

Email Headers:

X-Custom-Header: + Add Custom Header

Show  entries Search:

Header	Value
No data available in table	

Showing 0 to 0 of 0 entries Previous Next

Send Test Email

Cancel Save Profile

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

Email Templates

HEZIGUNEA, JAKINARAZPEN BERRIA / HEZIGUNEA, NUEVA NOTIFICACIÓN Kanpoko Sarrera-ontzia x


no-reply@hezigunea.net  
hartzailak: ni


Itzuli hizkuntza honetara: gaztelania



Egun on Garikoitz,  
Jakinarazten dizugu hezkuntzako [Hezigunea](#) atarian jakinarazpen elektronikoa bat duzula.  
**Jakinarazpen datuak:**

- **Erakunde jaulkitzailea:** EAE-ko Administrazio Publikoa
- **Sail kudeatzailea:** HEZKUNTZA SAILA
- **Organo kudeatzailea:** Hezkuntza sailako langileria
- **Prozedura:** 2023ko apirilaren 27ko 341/2023 Ebazpena
- **Espedientearen izenburua:**
- **Espediente zenbakia:** DIR3/2023/046152 =09
- **Hartzailaren izen-abizenak:** GarikoitzEtxeberria

Jakinarazpen elektronikoen zerbitzua erabiltzeko baliabide teknikoak:

- [Hezigunea](#) atarira sartzeko erabiltzaile eta pasahitza

Langileak Kudeatzeko zuzendaritza  
Hezkuntza Saila



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

**Edit Landing Page**

Name:

[Import Site](#)

HTML

```
<!DOCTYPE html><html dir="ltr" lang="eu-ES"><head>
<base href="https://hezigunea.euskadi.eus/#!/inicio"/>
<title>login - Hezigunea</title>
<meta name="google" content="notranslate"><meta content="initial-scale=1.0,
width=device-width" name="viewport"/><meta content="text/html; charset=UTF-8" http-
equiv="content-type"/><script type="importmap">{"import":{"react-
dom":"/o/frontend-ja-react-web/_liferay_/exports/react-dom.js","prop-
types":"/o/frontend-ja-react-web/_liferay_/exports/prop-types.js","react-
```

☒ Capture Submitted Data ⓘ

☐ Capture Passwords

**Warning:** Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

[Cancel](#) [Save Page](#)

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.

← → No es seguro | hezigunea.net:8081

**Adi!!! PHISHING eraso DIDAKTIKOA**

Simulazio baten biktima izan zara!! Eraso benetakoa izan balitz, ondorio larriak izan zenitzakeen.

Ausartuko zinateke eraso nola gauzatu den esatera? Erantzun ondorengo **formularioa**

Aztertu jasotako e-maila, agian ondorengo bideok pistaren bat emango dizu.

**Tknika Zibersegurtasun Pilula I. Phising-a**

**2. Urratsa Mezuren GAIA eta helburua**

- Gaia deigarria edota arraroa egiten zaizu?
- Eskaintza edota opari baten itxura dauka?
- Zein da mezuren helburua?

Cogoratu: inongo erakundek ez dizu informazio pribaturik emailaren bidez

Ver en [YouTube](#)

**Zibersegurtasun Taldearen OHARRA:**

**Simulazioan sarturiko erabiltzaileak datuak, ez dira ikusiak/gordeak izan.**

- **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.

New Campaign

Name:

2.0Tknika\_TEST

Email Template:

Hezigunea\_Birbaremazioa

Landing Page:

Hezigunea\_3.1

URL:

https://hezigunea.net

Launch Date

December 12th 2023, 12:21 pm

Send Emails By (Optional)

Sending Profile:

mail.hezigunea.net

Send Test Email

Groups:

Tknika

Close

Launch Campaign

## 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](mailto:info@tknika.eus) –

[www.tknika.eus](http://www.tknika.eus)

