

Tknika

KONTZIENTZIAZIO KANPAINAK





AURKIBIDEA

01

Helburuak

02

Smartfense

03

Edukiak

04

Lanketa

05

Pasahitz
seguruak

06

Phishing

07

Emaitzak

08

Ondorioak

Kontzientziazio kanpaina **ZERGATIK?**



Errealitate berri bat.
Malgutasunarekin batera
bulnerabilitateak



Informazioa, pasahitzak...lapurtzeko
helburuz, ohikoagoak dira berauek
eskuratzeko **erasoak**.





Edozein izan gaitezke erasotiak...

%95

Ziber-eraso kasu gehienetan
pertsonen ekintzak egoten dira
erasoen jatorrian



Kontzientziazioa

Arriskuen aurrean hezi. Praktika onak
bultzatu.



HELBURUAK

01

Kontzientziazioa

Langileak sarean dauden arriskuez kontzientziatu. Gure ekintzek ondorio larriak izan ditzakete datuen segurtasunean.

02

Formakuntza

Informazioa partekatzerakoan, korreo bat irekitzerakoan....praktika onak erakutsi.

03

Prebentzioa

Segurtasun neurriak hartu. Gure sistemak babestu eta lan ingurune seguru bat eraiki.

04

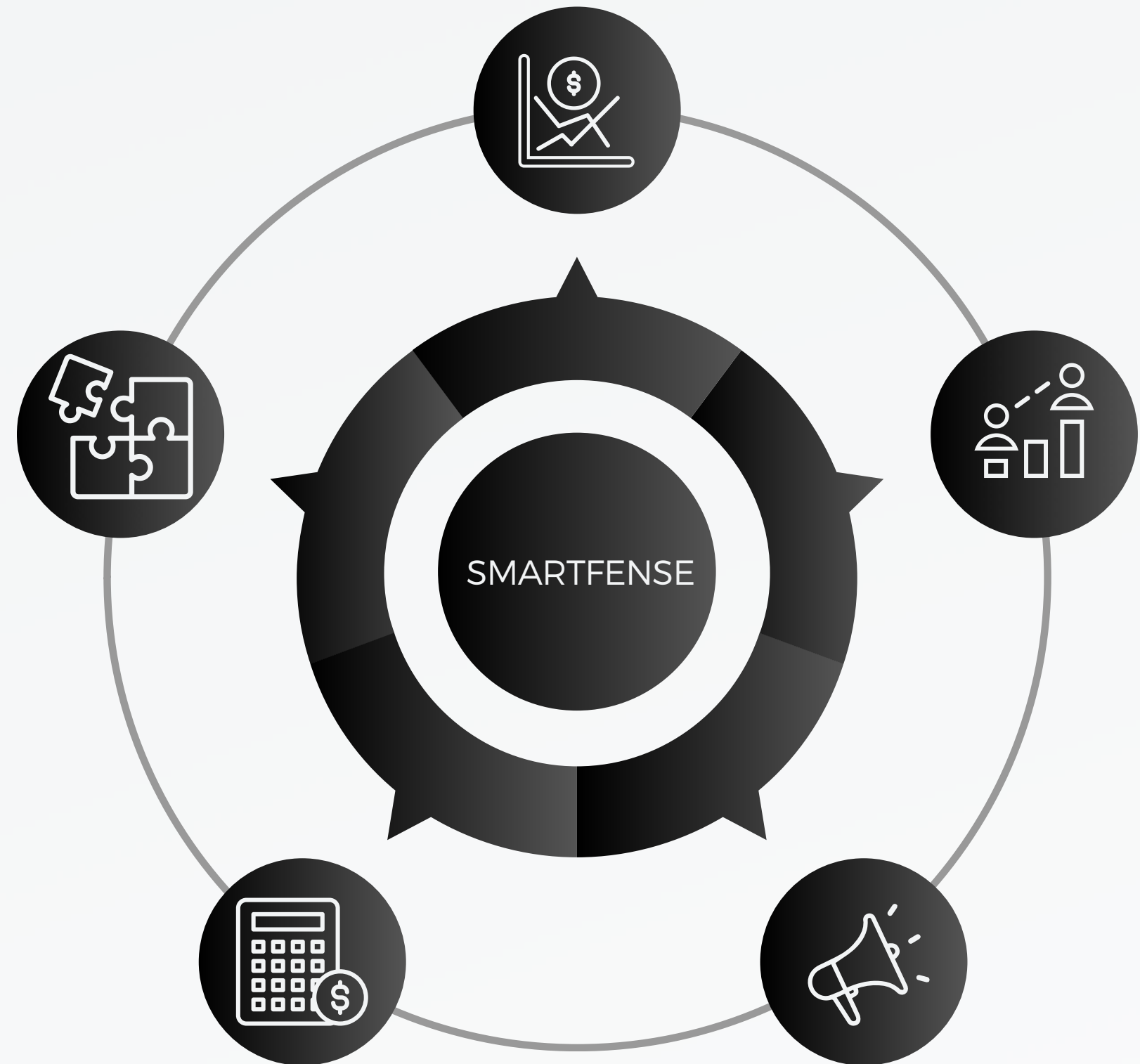
Mehatxuak

Saretik datozen arriskuak ezagutu. Phishing, ransomware...

05

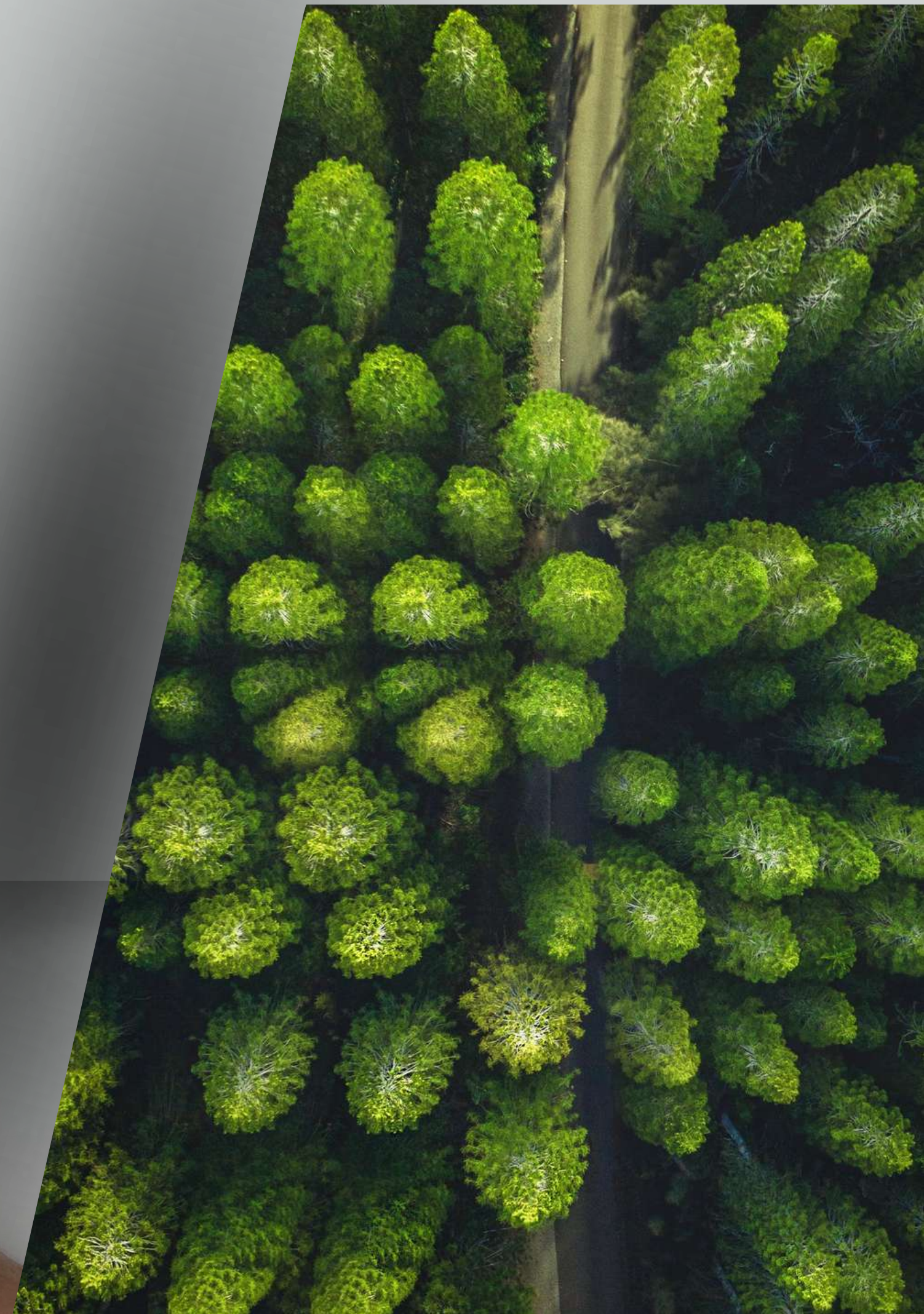
Ebaluazioa

Langileen jarrerak aztertu, hutsuneak detektatu eta hobekuntzak inplementatu.





**PASAHITZ SEGURUAK
PHISHING / RANSOMWARE**



SMARTFENSE

EZAUGARRIAK



Malgutasuna

Lizentzietan aukera zabala eskeintzen du. Langile ugari kudeatzeko, taldekatzeko erraztasunak. Gailu eta plataforma ezberdinak erabiltzeko aukera.



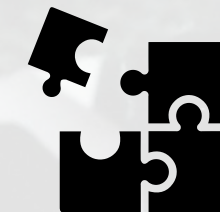
Aniztasuna

Eduki banku interesgarria. Mota ugaritako baliabideak. Modu erraz eta entretenituan edukiak partekatzeko aukera.



Emaitzak

Emaitzak jaso eta interpretatzeko erraztasunak. Grafikak, estatistikak...arrisku guneak ikusi, norbanako zein talde mailan.

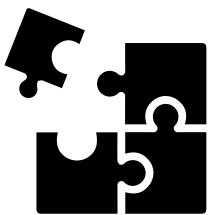


Euskara

Gure hizkuntzarekiko trataera ona. Itzulpen txukunak eta soporte bikaina hizkuntza guztiekiko.

EDUKI BANKUA

Modulu interaktiboak
Momentu edukatiboak



Phishing
Ransomware simulazioak

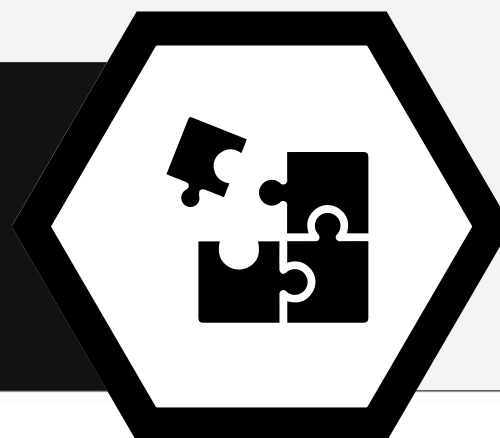
Bideoak
Newsletterrak




Azterketak
Inkestak

EDUKI BANKUA

Modulu interaktiboak Momentu edukatiboak



 Segurtasuna hodeian

SARRERA

Hodeian informazioa gordetzeko zerbitzuek gure fitxategietan edozein toki eta gailutatik sartzea, gure informazioa antolatzea, behar dugunean fitxategiak partekatzea eta hodeiarekin gure gailuan daukagun karpeta bat sinkronizatzea (lineako segurtasun kopia bat sortuz) ahalbidetzen digute.

Hala ere, batzuetan zerbitzu horiek eraso ditzakete edo segurtasun akatsak izan ditzakete eta ondorioz, arriskuan jar daiteke bertan gordetako informazio konfidentziala, baita zabaldu ere.

**Mezu elektronikoko
susmagarriak nola
identifikatu azaltzen
duten infografiak**



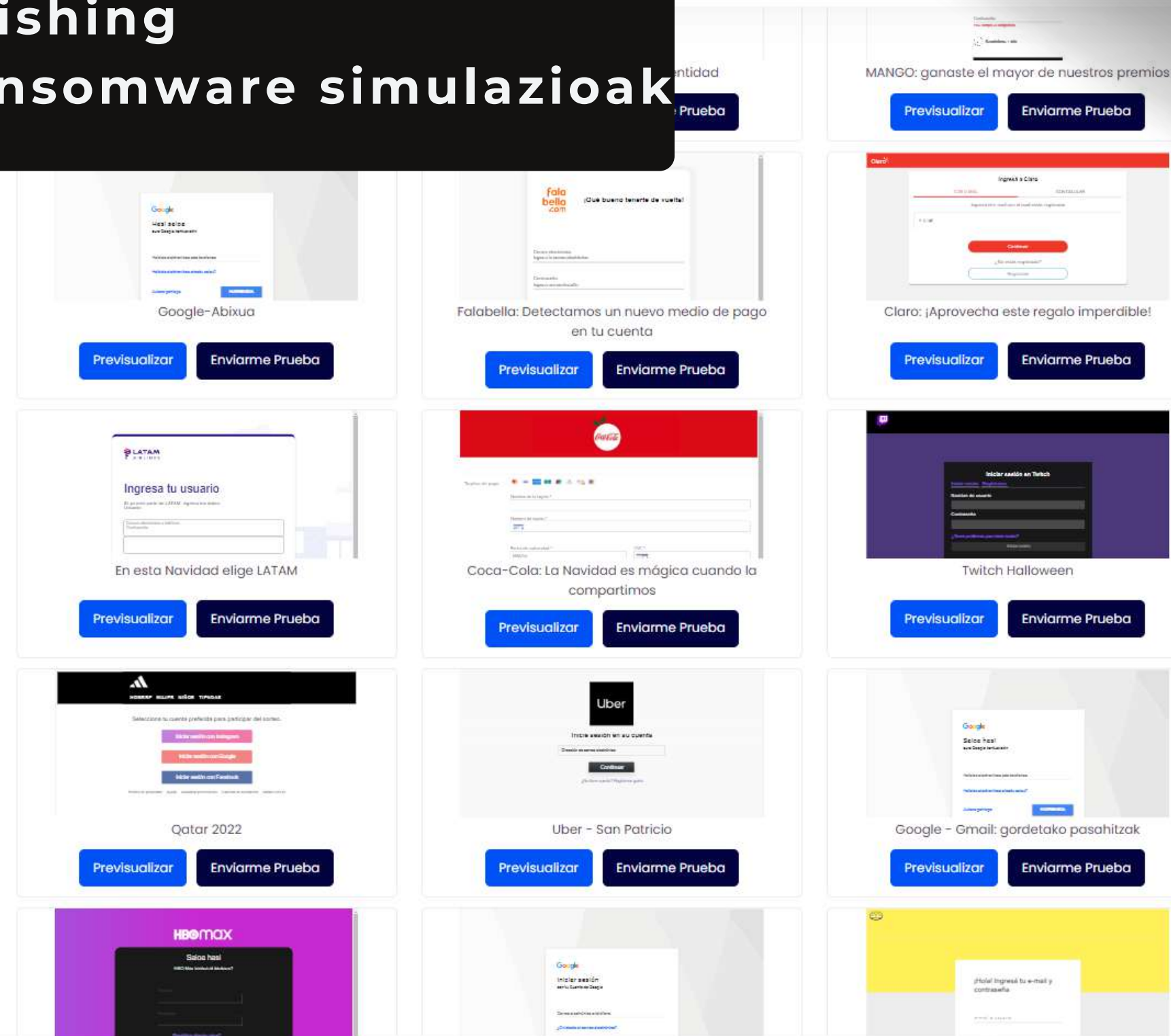
**Esteka eta erantsitako
fitxategi maltzurren
adibideak**

EDUKI BANKUA



Phishing Ransomware simulazioak

Probako mezu
elektronikoen bidalketa,
erabiltzaileen erantzuna
ebaluatzeko



EDUKI BANKUA

Bideoak
Newsletterrak



Informazio pertsonal
eta korporatiboa
babesteko azalpenak

MODU SEGURUAN NABIGATU INTERNETEN

Gaiak irakasteko saio
interaktiboak



 **SMARTFENSE**

EDUKI BANKUA



Azterketak Inkestak



Phishing: Posta elektroniko bidezko delitua

00:59:51

1/5



GALDERA

Posta elektronikoaz gain, zein beste teknologia erabili dezake zibergaizkile batek gu engainatzeko eta gure informazioa lapurtzen saiatzeko?

Posta elektronikoaz baino ezin diezagukete informazioa lapurtu.

Posta elektronikoaz gain, mezu laburrak ere erabili ditzake.

Urrutitik komunikatzeko bide oro erabili dezake, hala nola sare sozialak, mezu laburrak edo telefono deiak.

**Erabiltzaileen ezagutza
maila neurtzeko
baliabideak**

Tknika

LAN EGITASMOA

TKNIKAko 59 langileen artean sareko arriskuen inguruan prebentzioa sustatzeko kontzientziazio kanpaina burutzea.

59 langile



Kanpainaren
hasiera



Ebaluazioa



Aurkezpena eta
partekatzea



KANPAINAK

Otsailean eta Maiatzean banatutako bi epetan burutu da kanpaina.

Kanpaina 1

Pasahitzak



Askotariko zerbitzuetara sarbidea izateko gakoa dira pasahitzak. Pasahitz seguruak erabiltzeko prozedurak landu.

Kanpaina 2

Phishing/ Ransomware



Phishing-aren eta Ransomware-aren inguruko sentsibilizazioa sortzea. Erabiltzen diren iruzurren inguruko informazioa partekatu.

S

A

F

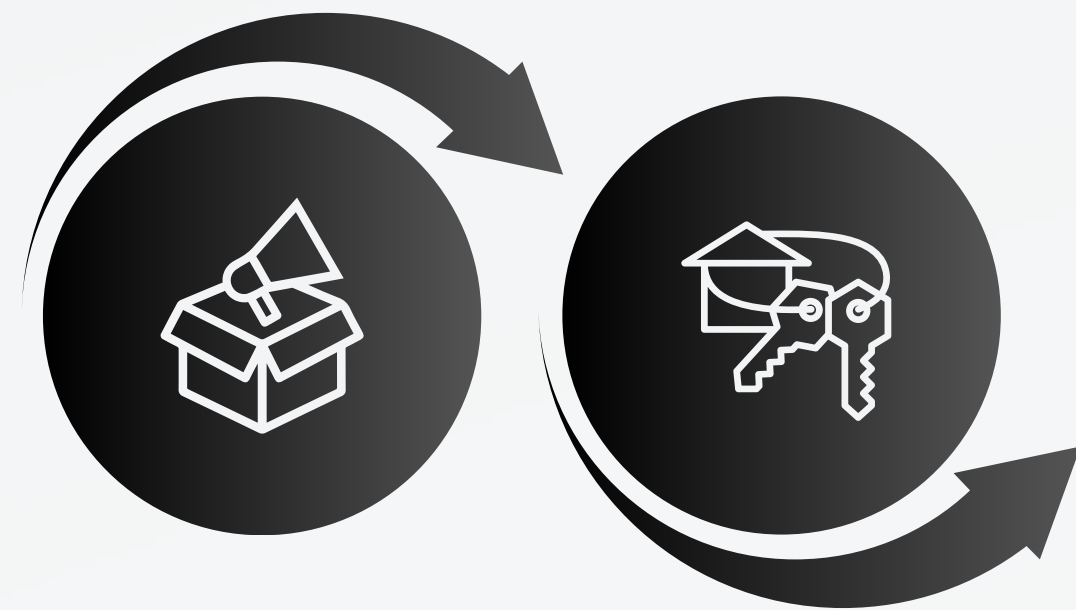
E

T

Y

Otsaila

Pasahitz seguruen
kontzientziazio
kanpaina. Baliabideak
partekatu.

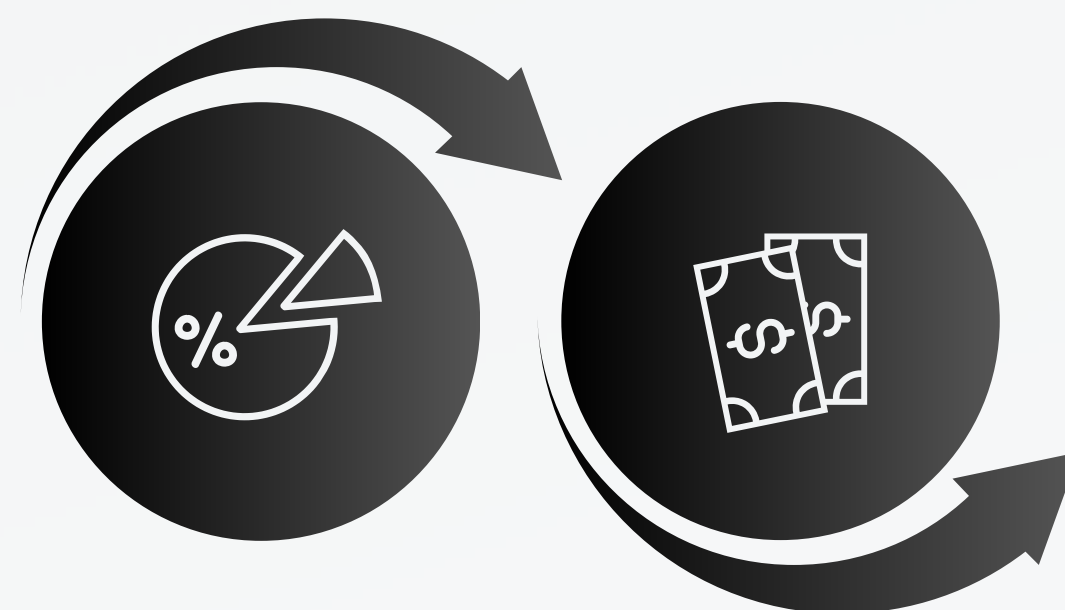


Urtarrila

Edukien prestaketa.
Kanpainen
denboralizazioa eta
baliabideen antolaketa.

Apirila

2.kanpainaren
prestaketa.
Phishing/ransomware
edukiak antolatu.
Bidalketak
denboralizatu

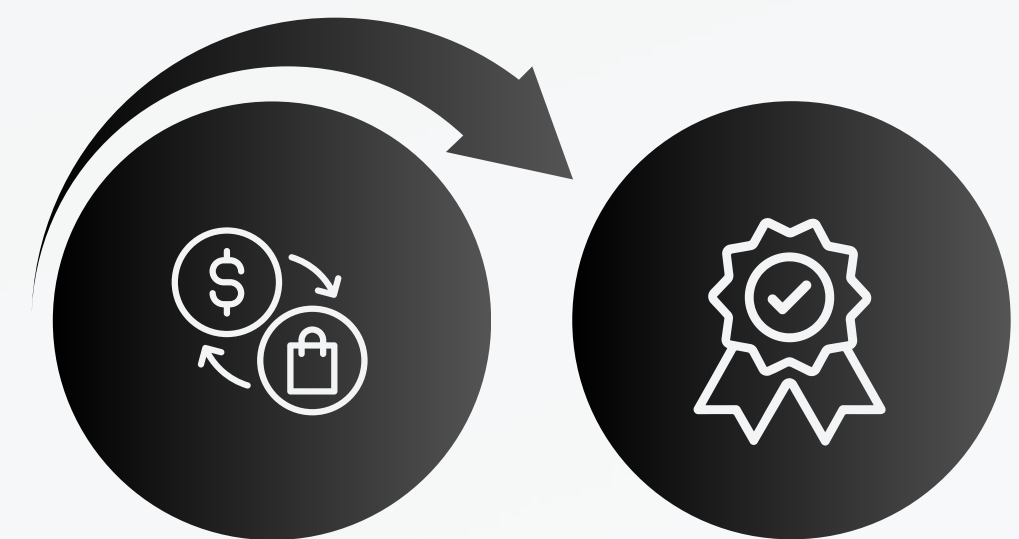


Martxoa

1.kanpainaren emaitzen
balorazioa. Izanadako
partehartzearen datuak
jaso.

Ekaina

Emaitzen diagnostikoa.
Partehartze datuak,
arriskuen ebaluazioa,
feedback lanketa.
Aurrera begirako
hobekuntza plana.



Maiatza

2.kanpainaren
exekuzioa. Phishing
iruzur mezuen
bidalketa. Baliabide
ezberdinak partekatu
informazio erantsia.

This example of
Single::ToString()
Single::ToString()
Single::ToString()
Single::ToString()
generates the following output when run in the console:
A Single number is formatted with various combinations of
strings and IFormatProvider.

IFormatProvider is not used; the default culture is for
No format string:
'N5' format string:
'E' format string:
'E5' format string:
A CultureInfo object for en-US is used for the IFormatProvider:
No format string:
'N5' format string:
'E' format string:
'E5' format string:

Tknika

PASAHITZ SEGURUAK





ESTATISTIKAK

NordPass erakundeak urtero **50 herrialdetako** erabiltzaileek gehien aukeratzen dituzten pasahitzen inguruan egindako ikerketaren emaitzak.

90% **AHULAK**



1.	password	4.929.113
2.	123456	1.523.537
3.	123456789	413.056
4.	guest	376.417
5.	qwerty	309.679
6.	12345678	284.946
7.	111111	229.047
8.	12345	188.602



8 **DIGITU**



Erabilitako **BALIABIDEAK**

Otsaila

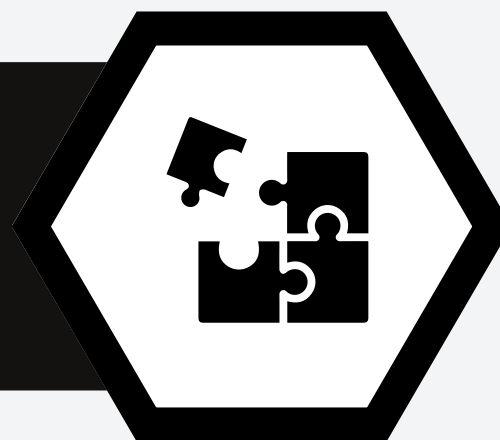
2 aste

- 1** Modulu interaktibo
- 1** Bideo
- 2** Newsletter
- 1** Azterketa
- 1** Bideojoko



LANDUTAKO EDUKIAK

PASAHITZ seguruak



Pasahitz **seguruak** erabiltzearen garrantzia azpimarratu.

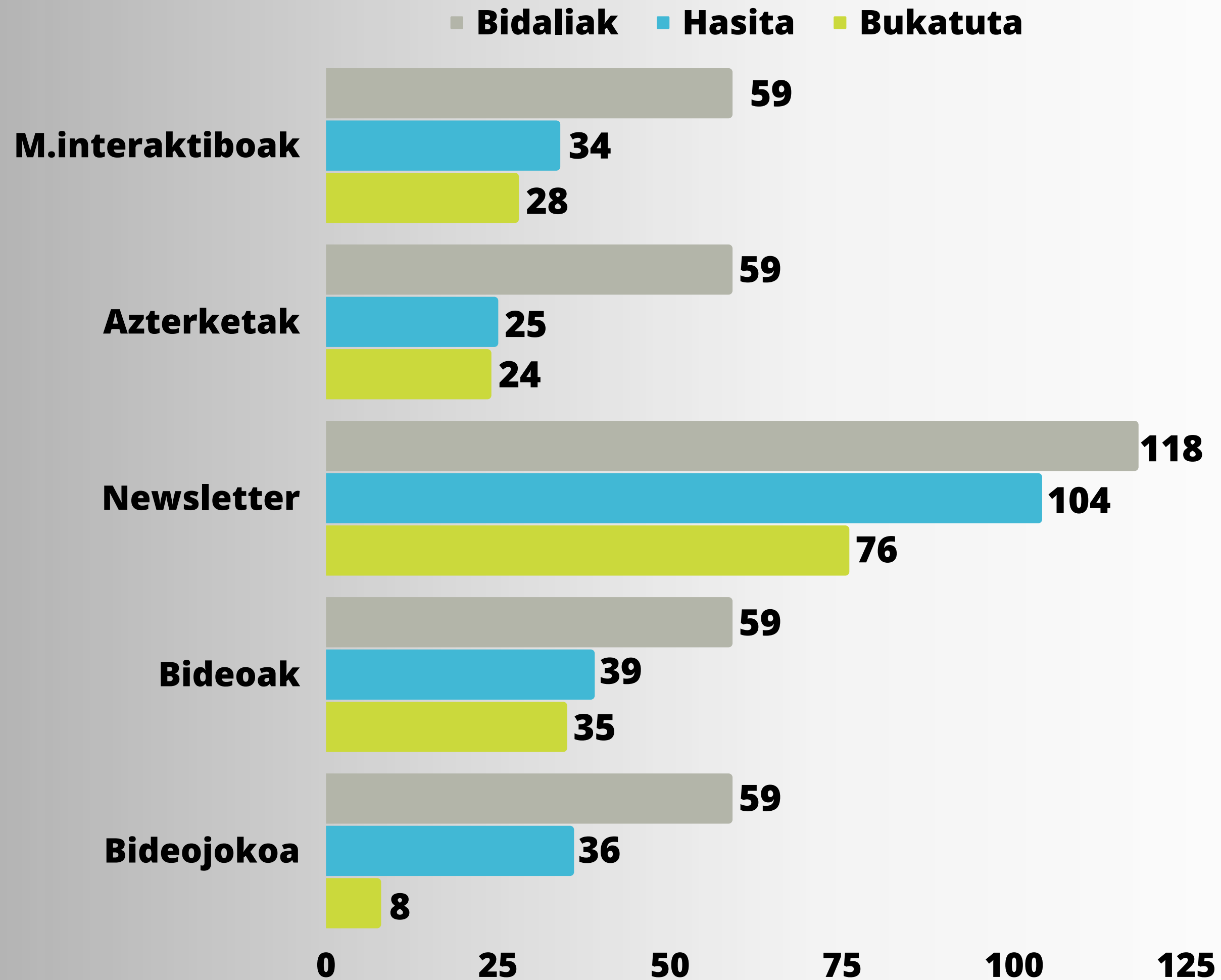


Lan eremuan langileek dituzten lan **ohiturak** aztertu.



Interaktiboki langileak **formatu** eta ondorioak ateratzeko ebidentziak lortu.





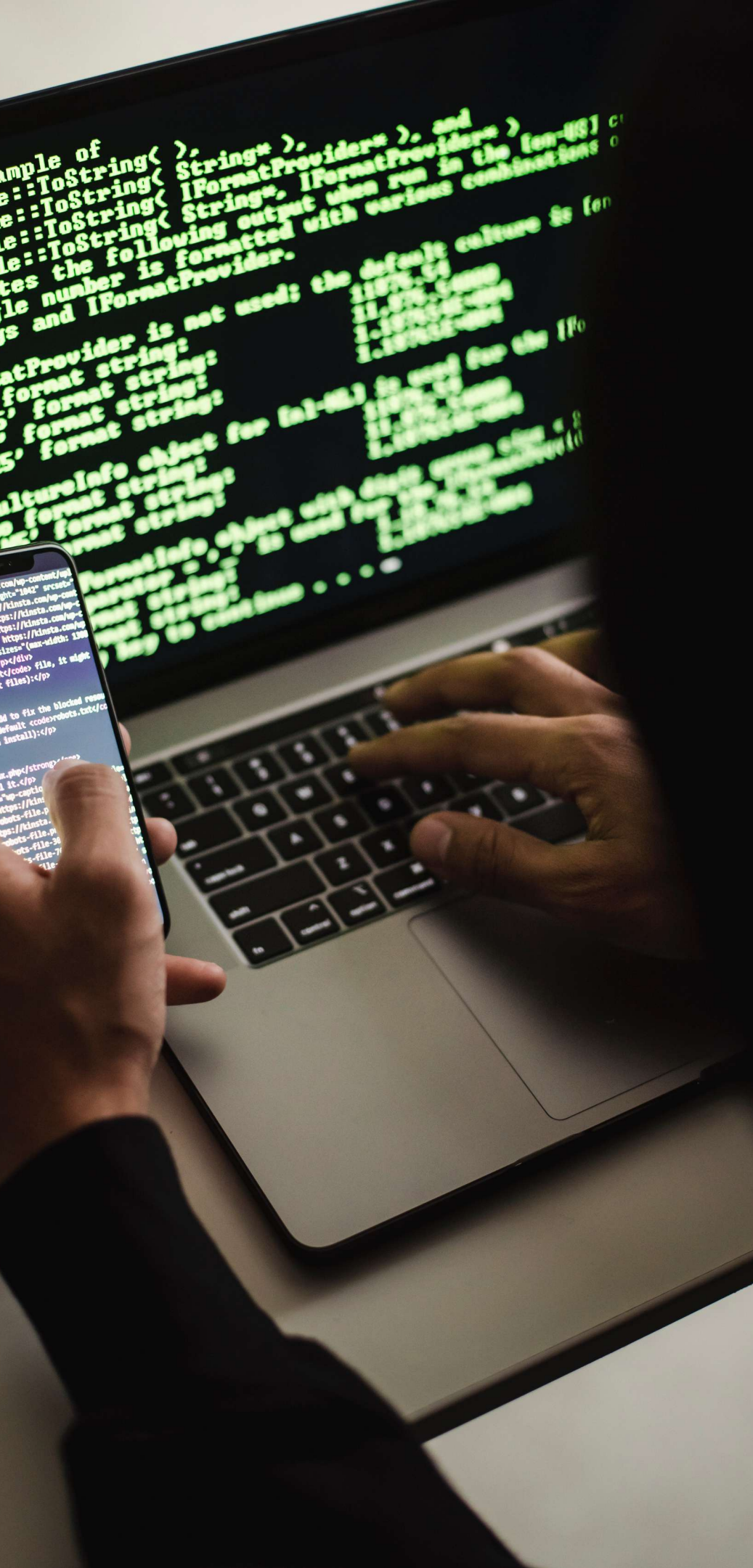
This example of
Single::ToString< String> //
Single::ToString< IFormatProvider>
Single::ToString< String, IFormatProvider>
Single::ToString< String, IFormatProvider>
generates the following output when run in the
A Single number is formatted with various combinations of
strings and IFormatProvider.

IFormatProvider is not used: the default culture is for
No format string:
'N5' format string:
'E' format string:
'E5' format string:
A Culture object for en-US is used for the IFormatProvider:
No format string:
'N5' format string:
'E' format string:
'E5' format string:

Tknika

PHISHING-RANSOMWARE

rc="https://kinsta.com/wp-content/uploads/2019/04/1390x1390.png" width="1390" height="1390" srcset="https://kinsta.com/wp-content/uploads/2019/04/1390x1390.png 1390w, https://kinsta.com/wp-content/uploads/2019/04/695x695.png 695w, https://kinsta.com/wp-content/uploads/2019/04/347x347.png 347w" sizes="(max-width: 1390px) 100vw, 1390px"/>
code>robots.txt</code> file, it might be robots.txt files):</p></div>



ESTATISTIKAK

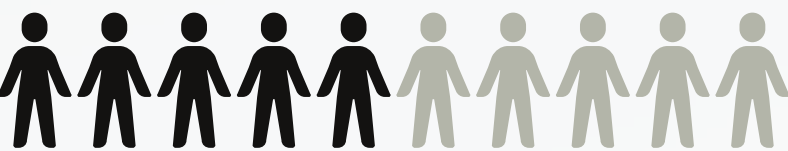


Egindako ikerketa baten arabera galdetutako enpresen **%83**ak onartzen du noiz edo noiz **Phishing** eraso arrakastatsu bat pairatu duela. **2022an %47,2** igo dira korreo elektronikoz eginiko eraso mota hauek.

83%



47% 



Erabilitako **BALIABIDEAK**

Maiatza **2 aste**

3

Modulu interaktibo

1

Bideo

1

Newsletter

2

Azterketa

1

Bideojoko

2

Phishing bidalketa

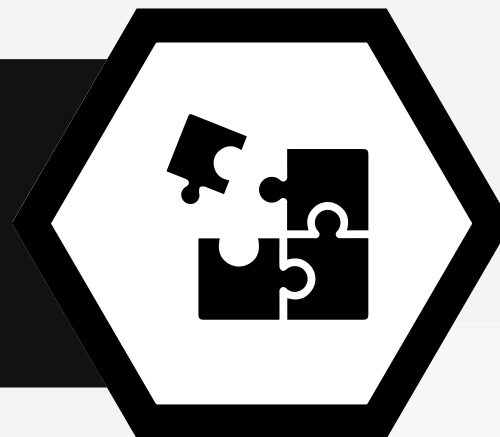
1

Ransomware bidalketa



LANDUTAKO EDUKIAK

Phishing Ransomware



Mezu "**pozoinduen**" bidalketa.



Momentu edukatiboak, erabilera txarra egin duten langileei zuzenduak.



Interaktiboki langileak formatu eta arriskuez prebenitu.



Saioa hasi

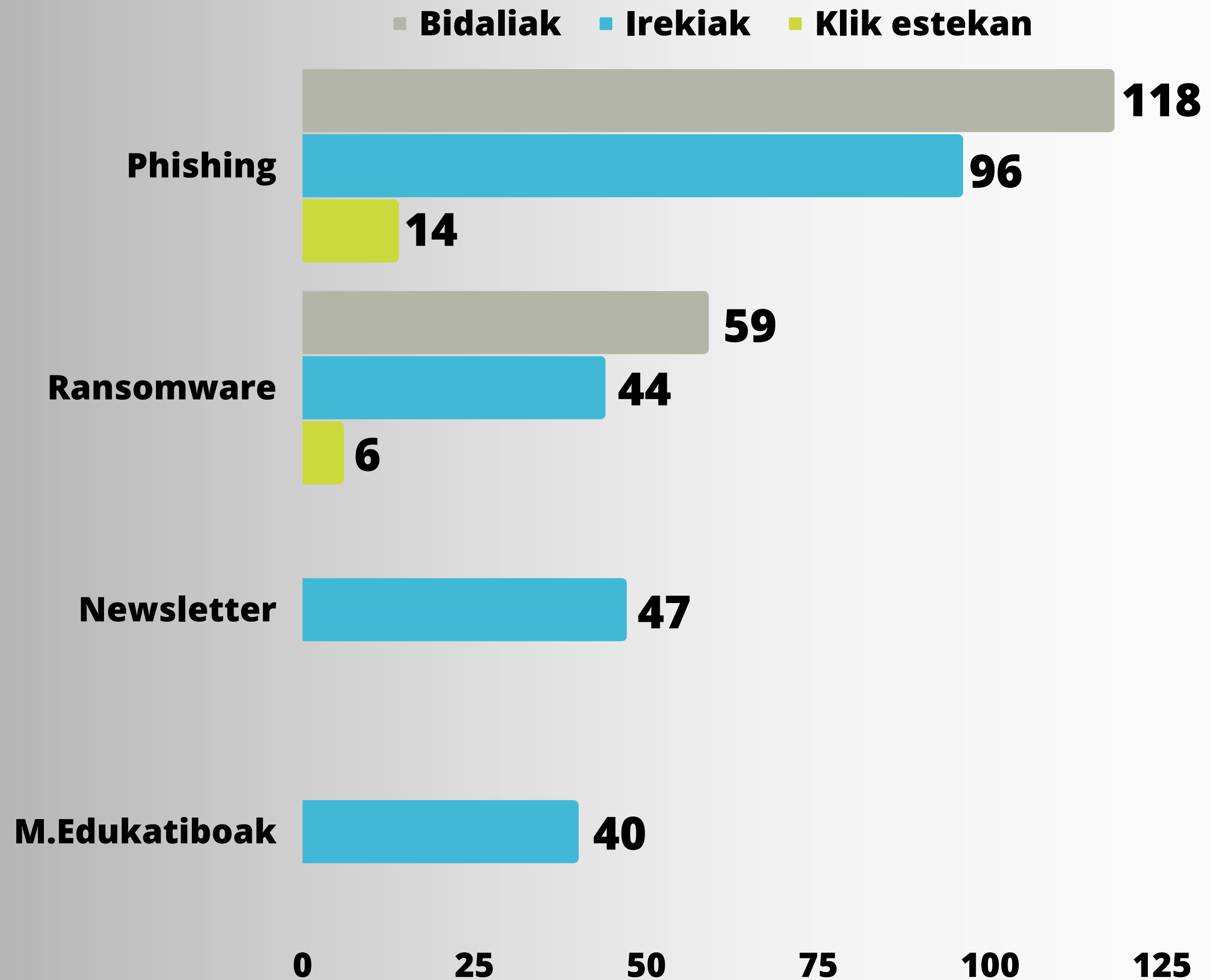
zure Google kontuarekin

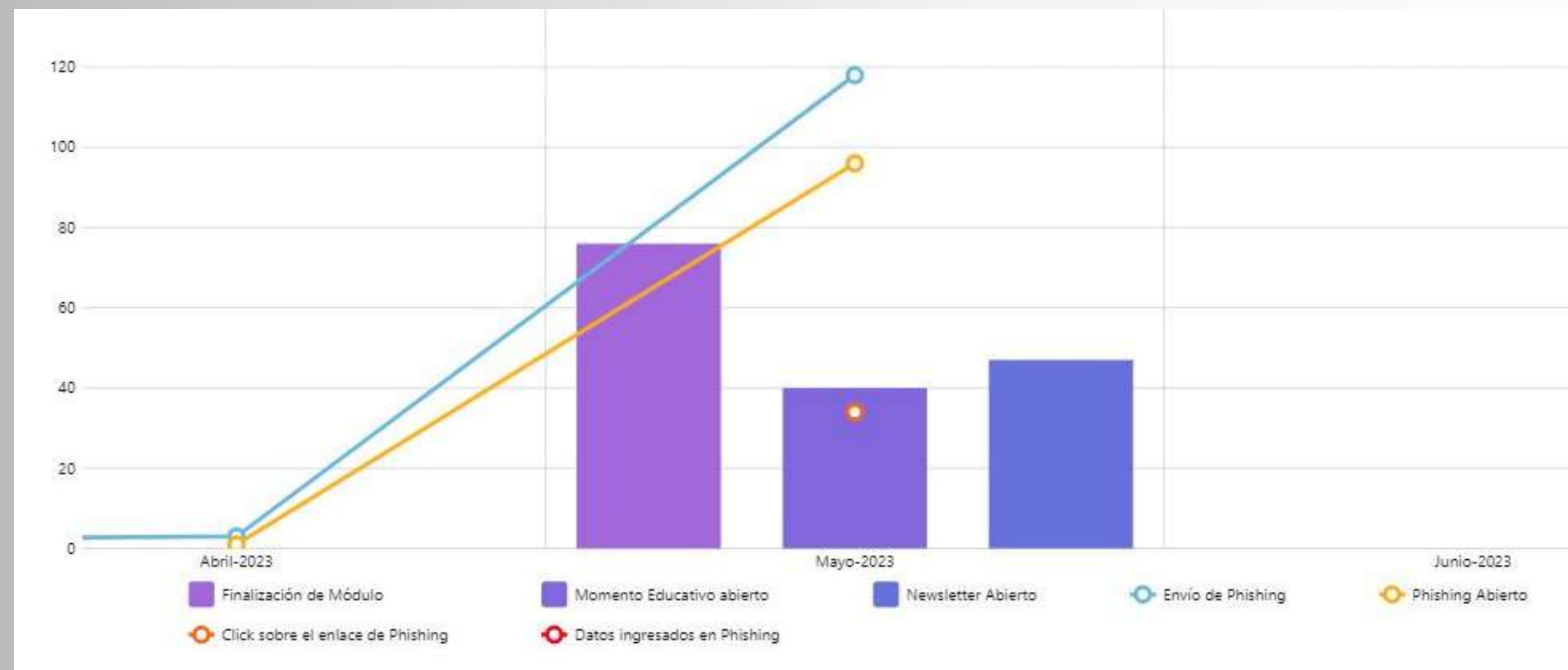
Helbide elektronikoa edo telefonoa

[Helbide elektronikoa ahaztu zaizu?](#)

[Aukera gehiago](#)

HURRENGOA





Arrisku maila

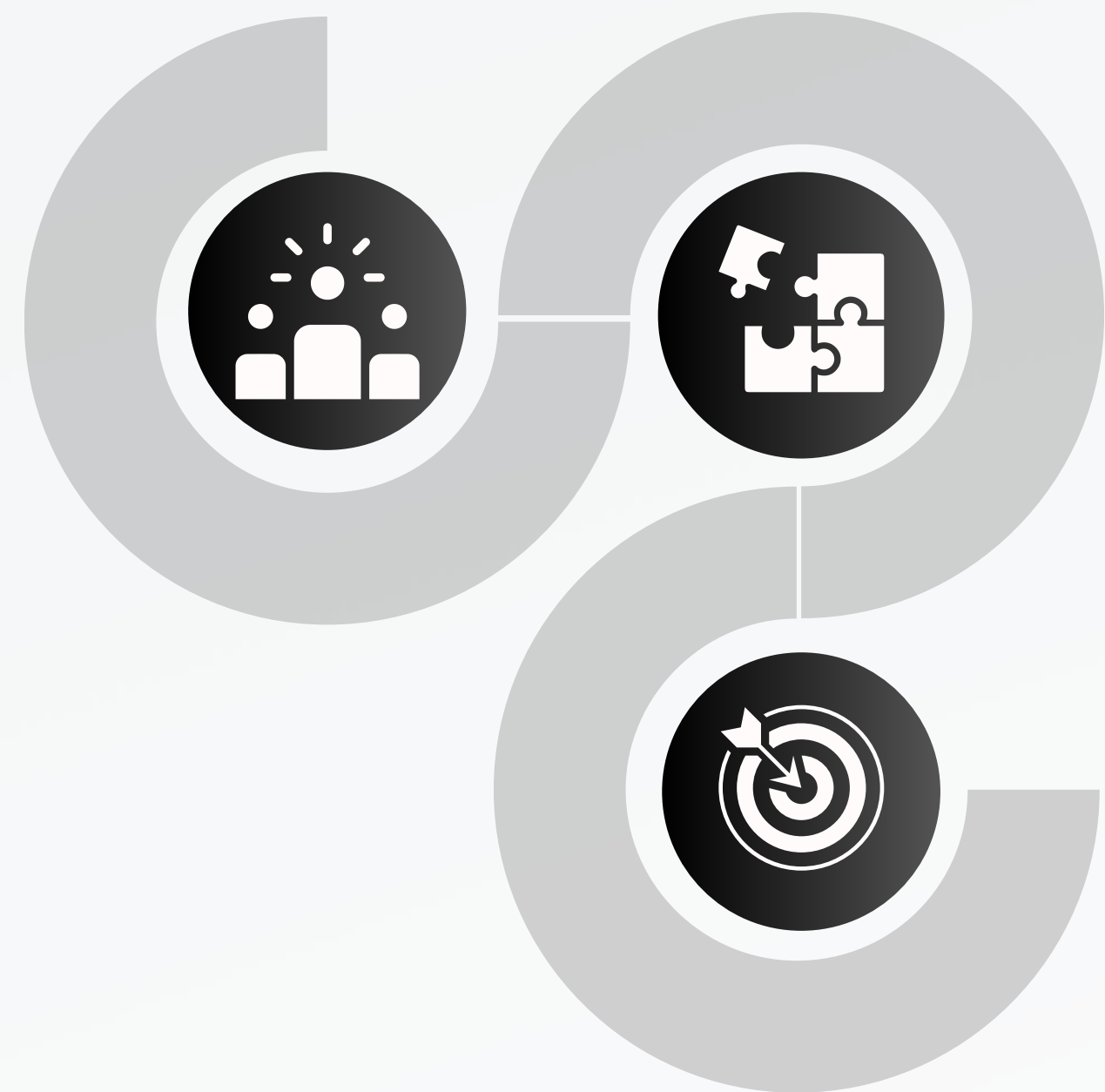
23%



ONDORIOAK

Tknika

- 01** Puntu ahulak aurreikusi eta bitartekoak bideratu.
- 02** Zaintza teknologikoan baliabideak inbertitu.
- 03** Giza ikuspegian ere bitartekoak. Kontzientziazioa eta formakuntza.
- 04** Etengabeko hobekuntza, mehatxu berrien bigilantzia
- 05** Partehartzea igotzeko. Aurrez komunikatu langileei eta zuzendaritzaren babesa lortu.



GoPhish

AN OPEN-SOURCE PHISHING TOOL

Beste aukerak...



Email Opened

Clicked Link

Submitted Data

Badaude aztertzea merezi duten tresna alternatiboak.



EASO Politeknikoa

GoPhish erabili dute beraien ikastetxean kontzientziazio kanpaina burutzeko.

Tknika

