TecnoCampus
Escola Superior
Politècnica

Centre adscrit a la
upf. Universitat
Pompeu Fabra
Barcelona

**Grau en Enginyeria Informàtica de Gestió i Sistemes d'Informació**

# ANÀLISI I DISSENY D'UNA WEB API DE DETECCIÓ DE PÀGINES PHISHING

**Memòria**

**MARC SERRA**
**TUTOR:LÉONARD JANER**

CURS 2021

TecnoCampus
Mataró-Maresme

## Agraïments

Al meu tutor Léonard Janer, pel suport, per les pautes i les guies rebudes en el projecte.

A la meva família i amics pel seu suport incondicional.

## Abstract

Currently the cybercrime industry is one of the most profitable and extended around the computing-information world. In this industry the electronic fraud knows as “Phishing” is one of the most increasing areas during last years. Due to little infrastructure necessary and ease of income making. This project addresses the problem, by investigating and analysing this line of cybercrime and with the objective to create a list of good practices-tips and a safe web platform for fraud detection.

## Resum

La industria del delicte informàtic és a dia d’ avui una de les més lucratives i difoses al món de la informàtica. En aquesta industria l’ estafa electrònica “*Phishing”* és una de les àrees que més ha crescut en els darrers anys. Degut a la poca infraestructura necessària i a la facilitat de generar ingressos. Aquest projecte aborda aquesta problemàtica mitjançant la investigació i l’anàlisi d’aquesta branca, amb l’objectiu de crear una llista de bones pràctiques per a la mitigació i la creació d’una plataforma segura de detecció de frau de pàgines web.

## Resumen

La industria del delito informático es hoy en día una de las más lucrativas y difundidas en el mundo de la informática. En esta industria la estafa electrónica “*Phishing*” es una de las áreas que más ha crecido durante los últimos años. Debido a la poca infraestructura necesaria y a la facilidad de generar ingresos. Este proyecto aborda esta problemática mediante la investigación y el análisis de esta rama, con el objetivo de crear una lista de buenas prácticas para la mitigación y la creación de una plataforma segura de detección de fraude de páginas web.

# Índex

# Índex de figures

# Índex de taules

# 1. Introducció

"*Hemos hecho tecnología para Leonard, para Sheldon, Rajesh, incluso Wolovitz (que al menos tiene un máster…) pero nos hemos olvidado de Penny. Hay que hacer seguridad para Penny, para el usuario corriente"*

*– Chema Alonso – Un informático en el lado del mal – CDCO Telefónica*[1]

## 1.1 Objecte del projecte

La problemàtica del delicte informàtic conegut com "Phishing" o frau electrònic afegeix la necessitat de generar una metodologia d'actuació, establir un codi de bones pràctiques, de cara al usuari amb la finalitat de conscienciar-lo i disminuir els afectats d'aquesta pràctica fraudulenta.

Aquest projecte tracta de resoldre aquesta problemàtica amb una plataforma web que identifica, analitza i estableix la perillositat d'una pàgina web i a més a més mitjançant la plataforma web crear una eina de divulgació amb l'objectiu d'alertar, mitigar i generar una llista de bones pràctiques al usuari no professional.

[1] José Maria Alonso Cebrián conegut com Chema Alonso és membre del Consell Executiu de Telefònica i conegut expert en ciberseguretat espanyol. La cita va ser comentada durant les jornades del Security Day a Madrid el maig de 2015.

# 2. Objectius i abast

## 2.1 Objectius del projecte

L'objectiu principal és fer un estudi del sector de la seguretat informàtica dirigida als atacs informàtics tipo *phishing* i crear un producte que resolgui la problemàtica de les pàgines *phishing* falsificades o malicioses. *(spoofing)*

## 2.2 Objectius del producte

Crear una pàgina WEB que analitza enllaços web, obtenint tota la informació possible per identificar la seva perillositat. Generant una mètrica numèrica o visual que es notifica al usuari.

## 2.3 Abast del projecte

El projecte ha de tenir un estudi de l'estat del art del sector Ciberseguretat i el atac informàtic tipus *phishing* i una pàgina web que serveixi al usuari com a plataforma per identificar pàgines perilloses.

## 2.4 Estructura del projecte

El projecte està dividit en dues parts principals.

La primera part és d'investigació, anàlisi i estudi del art del sector.

La segona part és de desenvolupament i implementació d'una pàgina web que resolgui la problemàtica establerta.

## 2.5 Rols del projecte

El projecte està definit amb dues parts la d'estudi de l'estat i anàlisi de l'art del sector i la creació de la plataforma que soluciona la problemàtica. Per tant, existeixen diversos rols dins del propi projecte i diferent metodologia de treball.

Rols de gestió i control del projecte:

- Gestor de projectes

Rols en l’estudi del sector i estat de l’art:

- Investigador
- Analista i assessor de seguretat informàtica.

Rols en el desenvolupament de la plataforma web:

- Enginyer de sistemes d’informació.
- Dissenyador informàtic
- Programador
- Administrador de sistemes d’informació.
- Tester

# 3. Marc Teòric

## 3.1 Context

### 3.1.1 El món de la Ciberseguretat

La ciberseguretat o seguretat informàtica és la branca de la informàtica que estudia com protegir els sistemes informàtics, les xarxes de telecomunicacions, la informació i l'usuari contra qualsevol tipus d'atac, ja sigui de manera física, virtual o electrònica.

En el camp de la ciberseguretat existeix un risc constant d'atac anomenat *phishing*, és un dels mètodes d'atac més utilitzats mundialment i és una de les tècniques més estudiades en el sector.

### 3.1.2 Què és el *Phishing*?

El *phishing* es defineix com l'activitat criminal informàtica que utilitza l'engany mitjançant medis informatitzats i tècniques de psicologia social. Utilitzant la suplantació d'identitats, l'estafa, la persuasió i mala fe amb l'objectiu d' obtenir recursos econòmics, de la informació i/o causar danys a la propietat o la persona.

L'origen del terme és del anglès *Fishing* "Pescar". Va ésser adoptat el 2 de gener de 1996 per un grup d' usuaris anomenat *AOHell*[2]. *AOHell* va implementar una eina de *hacking* anomenat *Fisher* que permetia accedir a contrasenyes i informació bancària mitjançant la plataforma *AOL* d' enviaments de correu i comunicació.

El terme s'origina per què l'activitat principal del *phishing* és la de fer caure a la víctima a la trampa, "*bite the trap",* mossegar l'ham.

### 3.1.3 La tècnica del *Phishing*

En la tècnica del *phishing* no existeix un mètode únic de funcionament. Ja que l'objectiu principal és aconseguir el màxim benefici de les víctimes, per tant, la quantitat de tècniques existents augmenten dia a dia. També està en constant evolució, tant tecnològic com

[2] AOHell era una aplicació que s'utilitzava per aprofitar les vulnerabilitats de l'aplicació de correu electrònic AOL. (American Online)

metodològic, pel que fa difícil mantenir un llistat de tècniques completament actualitzades i fidels.

Però es pot entendre que l'eina principal per l'ús eficaç del *phishing* és l'enginyeria social. L'enginyeria social a l'àmbit del *phishing* té com objectiu adaptar l'atac a la víctima. És a dir, utilitzar la psicologia del propi usuari contra ell mateix, persuadir, manipular o coaccionar ja sigui amb informació externa o interna.

### 3.1.4 Les sis claus bases de l'enginyeria social

L'enginyeria social estableix sis punts claus que s'utilitzen tant al *phishing* com a gran part de l'àmbit de la ciberdelinqüència, ja sigui, perquè s'utilitzen una de les sis claus o la combinació de qualsevol de les sis. (Stamp) (Anderson, 2008) Aquestes són:

- Reciprocitat - *Reciprocity:*
    - Confiança i la voluntat d'ajudar als demes. Viure en una societat que es basa en la confiança. (*Trusting*) Els *hackers*[3] utilitzen aquesta tècnica per oferir consells, ajudes o favors com a mostra de confiança.
    - Exemple: L'atacant es fa passar per un amic de la víctima demanant el cobrament d'un favor o exigint que utilitzi un enllaç o un programa.
- Compromís – *Commitment:*
    - Voluntat de mantenir la paraula. Els *hackers* l'utilitzen per coaccionar a l'usuari perquè accedeixi a contractar serveis o subscripcions.
    - Exemple: L'atacant utilitza informació extreta de l'entitat víctima exigint el compliment d'un contracte o subscripció. L'entitat es veu forçada a accedir per tal de no perdre un client o possibles repercussions econòmiques.
- Socialment acceptat – *Social Proof:*
    - Pressió o acceptació social. Els *hackers* aprofiten aquesta tècnica perquè l'usuari cregui que és quelcom socialment acceptat, que tothom fa.
    - Exemple: L'atacant aprofita la informació extreta de xarxes socials per coaccionar a la víctima perquè utilitzi o es descarregui una aplicació.

[3] Un Hacker o furoner/a és una persona amb coneixement de sistemes informàtics que té com objectiu trobar vulnerabilitats dels sistemes d'informació, informàtics o de la telecomunicació però que no actua amb ànima criminal.

- Autoritat – *Authority:*
    - Exercir el poder de l'autoritat. El *hacker* aprofitarà una veu o figura autoritària per coaccionar a la víctima per tal de guanyar-se la confiança.
    - Exemple: L'atacant es fa passar per inspector de l'agència tributària, assegurant que l'entitat víctima ha sigut identificada per irregularitats. Posteriorment la víctima accedeix a pagar una retribució perquè no hi hagi repercussió o altres conseqüències.
- Agradar – *Liking:*
    - La voluntat d'agradar als demes. Aquesta tècnica és semblant a la d'autoritat però la diferència és què no s'utilitza una veu a figura autoritària sinó una d'influència o amistat.
    - Exemple: L'atacant utilitza informació de persones properes a la víctima i aconseguir beneficiar-se de la posició de favor. Així la víctima està disposada a proporcionar diners o informació.
- Limitat – *Scarcity*:
    - Limitació d'accés o escassetat. Aquesta tècnica vol generar una necessitat a l'usuari per accedir a la informació, ja sigui desorientant l'usuari, amagant la informació o generant sensació d'urgència.
    - Exemple: L'atacant modifica la lectura i/o l'accés a fitxers, informació, de la víctima de manera que aquesta accedeixi a proporcionar diners o informació.

### 3.1.5 Estudi de les tècniques

A partir de l'ús de l'enginyeria social es pot generar un atac *phishing amb* quatre tècniques més reconegudes:

- Email Spoofing
- Typo squatting
- Malvertising
- IDN homograph attack

**Email Spoofing**

Falsejament d'identitat anomenat *spoofing* és la tècnica que pretén suplantar la identitat d'un tercer amb la finalitat d'accedir a la informació de la víctima.

En aquest cas l'emissor de correu electrònic suplanta una entitat o persona mitjançant la falsificació de l'origen. D'aquesta manera pot falsejar les seves dades i comunicar al servei de correu de la víctima que està enviant un missatge amb unes credencials, tot i que en realitat no sigui així.

Com es pot observar a la Figura 3.1.1 hi ha l'exemple d'un correu electrònic amb credencials falsificades. El missatge tot i arribar de service.outlook.com és un correu falsificat, ja que el domini service.outlook.com del correu pertany a un domini falsificat de l'atacant i no a Microsoft outlook.com. D'aquesta manera l'atacant dona a entendre a la víctima que és un domini de confiança i així fer que la víctima accedeixi a l'adreça adjunta i aconseguir les seves credencials i contrasenya. (Microsoft Anti-spoof, 2021)


**Figura 3.1.1: Exemple d'un correu electrònic amb credencials falsificades.**

### Digital Impersonation

Aquesta tècnica és coneguda com falsejament o robatori d'URL. L'objectiu principal és registrar dominis web semblants a les organitzacions o entitats que es volen suplantar. Aprofiten diferents errors de les víctimes per tal de que accedeixin però en veritat tenen petites variacions de domini. (Fraud Magacine, 2013)

### Typo squatting

Aquesta tècnica es coneguda com l'error d'ortografia. Utilitza errors mecanogràfics per confondre a la víctima.

En la Figura 3.1.2 podem observar alguns exemples de la tècnica i els errors d'ortografia en alguns casos quasi imperceptibles.

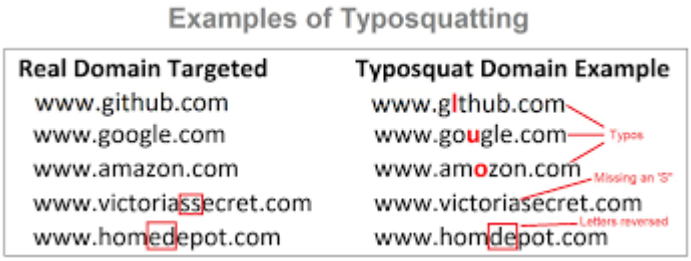


Figura 3.1.2: Exemples de typo squatting origen HENNES Communications.

La tècnica inclou en alguns casos com faltes d'ortografia, errors d'escriptura i errors deguts a la distribució del teclat.

### IDN homograph

Aquesta tècnica és coneguda com un atac homogràfic ja que l'objectiu és emmascarar una pàgina web il·lícita als navegadors d'internet codificant els nom dels dominis web per paraules o caràcters homògrafs, és a dir, que són semblants però no són el mateix.

En la Taula 3.1.1 tenim caràcters homògrafs de llenguatge ciríl·lic a llenguatge llatí, utilitzats com exemple de "apple.com", però que podem observar que en realitat tenen codificació , en *UNICODE*[4], diferent.

| Fake "apple.com" | | | Real "apple.com" | | |
|---|---|---|---|---|---|
| **Glyph** | **Unicode Name** | **Unicode Hex** | **Glyph** | **Unicode Name** | **Unicode Hex** |
| a | Cyrillic small letter A | U+0430 | a | Latin small letter A | U+0061 |
| p | Cyrillic small letter Er | U+0440 | p | Latin small letter P | U+0070 |
| ӏ | Cyrillic small letter Palochka | U+04CF | l | Latin small letter L | U+006C |
| e | Cyrillic small letter Ie | U+0435 | e | Latin small letter E | U+0065 |

Taula 3.1.1: Una taula d'exemples de lletres homògrafes.

[4] UNICODE és un estàndard de codificació de caràcters informàtic en format de unificat de de quatre valors hexadecimals. U+0000 a U+FFFF.

### Malvertising

El *Malvertising* és la tècnica que més ha augmentat els últims anys degut a la implantació del comerç electrònic i les xarxes socials a la vida quotidiana. Els atacants registren anuncis fraudulents amb l'ànima d'atraure la víctima.

El funcionament bàsic és el de registre d'un domini web fraudulent tipo *spoof* i redirigir l'activitat d'altres entitats cap aquesta pàgina mitjançant l'ús de anuncis a plataformes web de cerca.

En la Figura 3.1.3 podem observar el funcionament d'aquest tipus d' atacs amb el cas de descàrrega de *malware*[5].

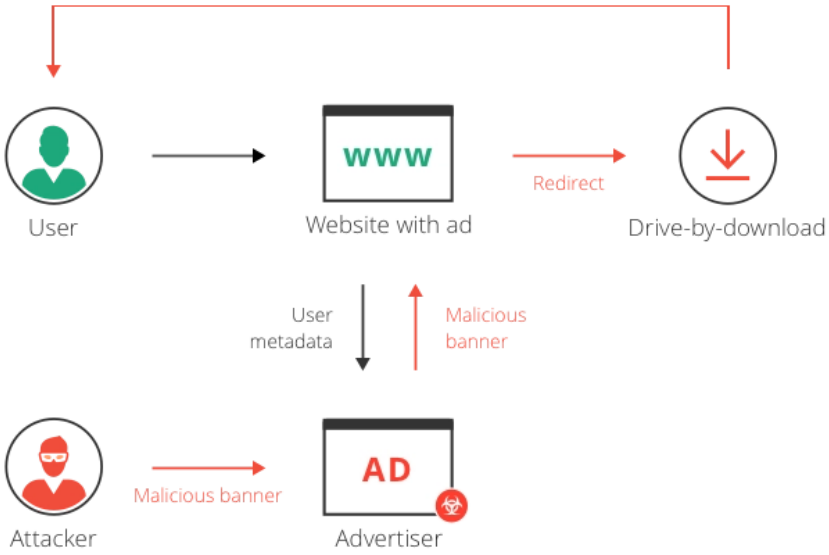


**Figura 3.1.3: Exemple del funcionament de Malvertising.**

La Figura 3.1.4 és un exemple de *Malvertising* amb l'objectiu d'obtenir informació de targetes de crèdit Mastercard. Es pot observar que l'anunci es mostra al cercador amb la paraula Mastercard però l'URL de l'anunci no coincideix amb el domini de la entitat.

[5] El *malware* és conegut com el programari perillós. Normalment són programes que tenen com objectiu obtenir informació o beneficiar-se de la víctima mitjançant l'ús dels recursos del sistema.

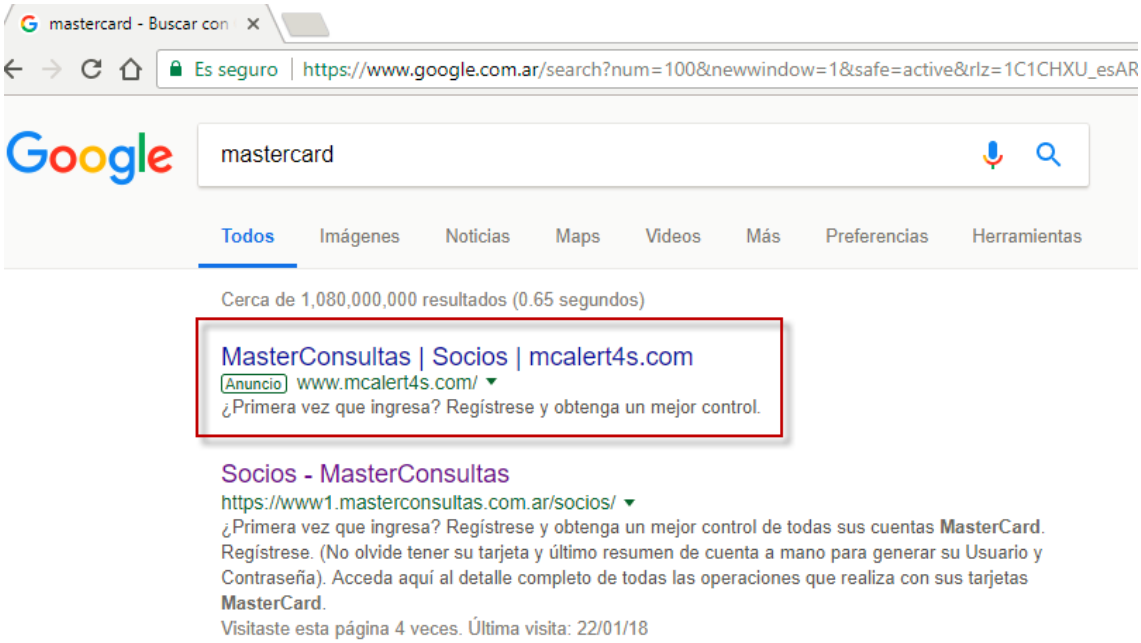


Figura 3.1.4: Exemple de Malvertising en un anunci de Google.

A la Figura 3.1.5 es pot observar on porta aquesta URL i es pot comprovar que és una replica fraudulenta (*web spoofing*) de la pàgina de targetes de crèdit Mastercard. Posteriorment a la figura 6 es demana la informació personal de la targeta de crèdit. (We live Security, 2018)

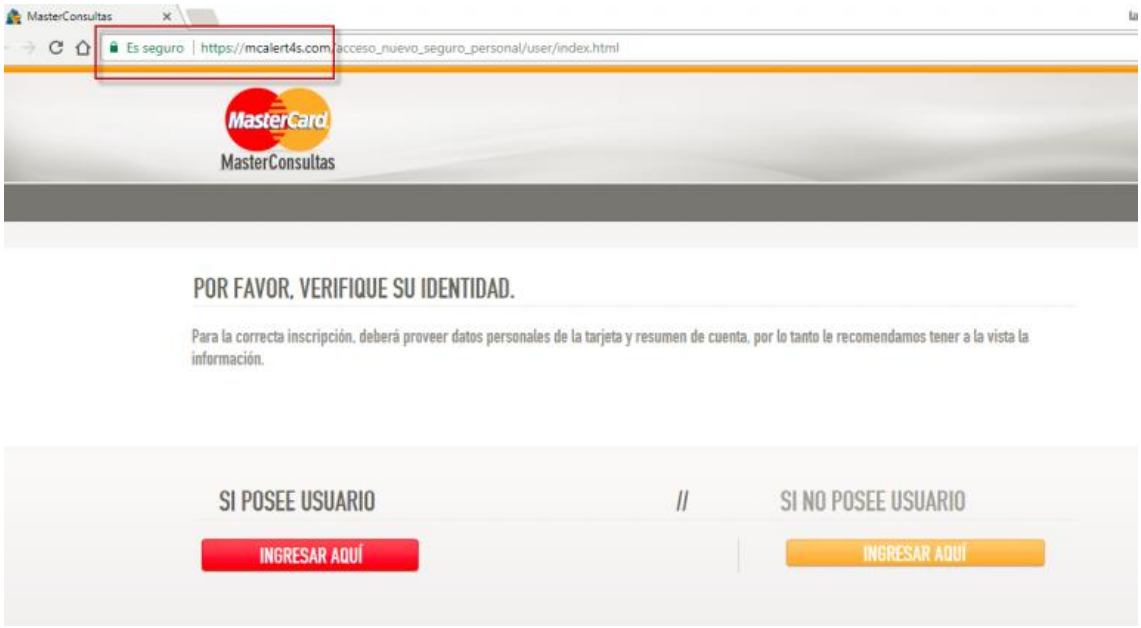


Figura 3.1.5: Enllaç de destí del anunci de Google de Mastercard.

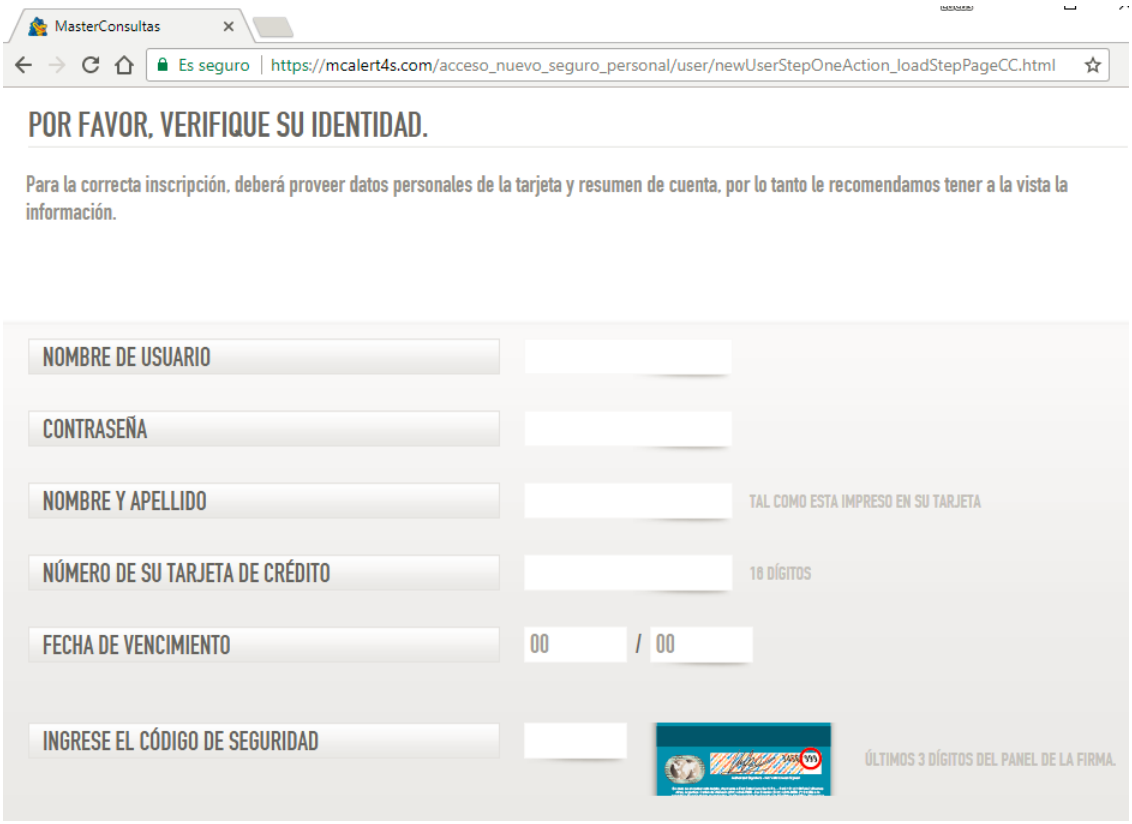


**Figura 3.1.6: Formulari de petició fraudulenta informació targeta de crèdit.**

Aquesta tècnica té la particularitat de que encara que sigui la més visible és la que registra més víctimes. La seva operativitat és curta ja que les plataformes, les entitats i els usuaris acostumen a alertar en poc temps de la falsedat però té una gran efectivitat.

### 3.1.6 Tipus de *Phishing*

**Email Phishing**

Email *Phishing* es tracta del més comú de tots i el més estès. La víctima normalment rep un correu electrònic obté informació, intenta realitzar una transacció econòmica i en alguns casos implantar *malware* al terminal.

És un dels tipus de fraus més habituals i més reconegut per l'usuari. Existeixen quatre classificacions:

- Deceptive Phishing
    - És el conegut com el que un *phisher* envia un correu normalment i es fa passar per una empresa o entitat coneguda per la víctima. Poden ser entitats financeres, empreses de logística o del propi sector.

- Spear Phishing
    - És el mateix que el *deceptive phishing* la diferència és que aquest va completament dirigit a la víctima. Ja sigui utilitzant informació externa o utilitzant eines de extracció de noms.
        - Exemple: antonio.s.54@transportadores.es

  "Sr. o Sra. antonio,"
- Whaling
    - Anomenat *whaling* pel mot anglosaxó *whale* "balena". Aquesta estafa està dirigida alts càrrecs d'empreses. Normalment s'utilitza la informació per fer xantatge. *(blackmailing)*.
- Bulk Phishing o directed spam
    - És el mètode més invasor. L'atacant enviarà de manera massiva al usuari o diversos usuaris molts correus amb l'objectiu d'inundar la bústia i/o evitar que la víctima pugui utilitzar-la de manera normal.

**Phishing de xarxes socials**

És una variant del *phishing* que ha crescut molt en els últims anys. Es tracta de l'utilització d'anuncis, campanyes i/o etiquetes a les xarxes socials on l'atacant aprofita aquestes plataformes per atraure a les víctimes a pàgines fraudulentes.

**Malware-based:**

Aquesta variant té com objectiu instal·lar software maliciós a la víctima. Ja sigui mitjançant descàrregues que pugui fer l'usuari de la xarxa, *scripts* o macros.

Software maliciós més comú en el *phishing*:

- *Ransomware:* encripta fitxers de la víctima impedint l'operativitat total o parcial del seu entorn fins que es faci una transacció, habitualment econòmica.
- *Adware:* afegeix software als navegadors d'internet amb l'objectiu de capturar dades de navegació de la víctima amb l'objectiu de vendre aquest contingut o utilitzar-lo contra la víctima.
- *Trojan horse*: és un software que suplanta o disfressa de software lícit amb l'objectiu d'obtenir control del terminal. Ja sigui per capturar informació o inhabilitant l'operativitat.

- *Worms:* és un software que busca vulnerabilitats dels sistemes operatius amb la finalitat d'instal·lar *backdoors* "portes posteriors" i accedir a la xarxa de la víctima.
- *Rootkits:* és molt semblant a la tècnica tipo *worms* però l'objectiu principal es prendre control d'administració a la xarxa de la víctima.
- *Keyloggers*: és un software que monitoritza l'activitat del teclat o dispositius d'entrada de la víctima.
- *Zero Days – Exploits:* aquest no es troba implícit en els atacs tipo *phishing* però pot ser una conseqüència d'un atac. Tracta de trobar vulnerabilitats no detectades en les versions dels sistemes o aplicacions de la víctima.

En la Figura 3.1.7 podem observar una llista dels deu primers softwares maliciosos el primer trimestre de 2019, on podem trobar alguns dels programes esmentats.

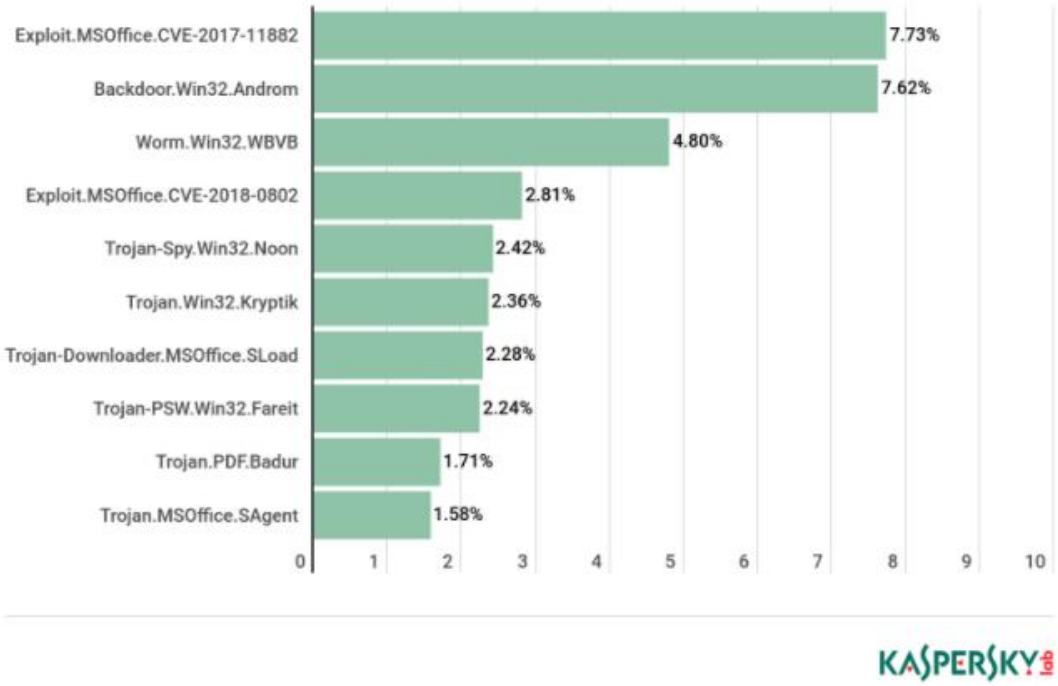


**Figura 3.1.7: Taula de dades dels deu primers software maliciosos enviats mitjançant correu electrònic 2019T1.**

### Cloning

Aquesta variant utilitza software de clonació de pàgines web amb l'objectiu d'enganyar a les víctimes per que utilitzin el portal web.(Figura 3.1.8)

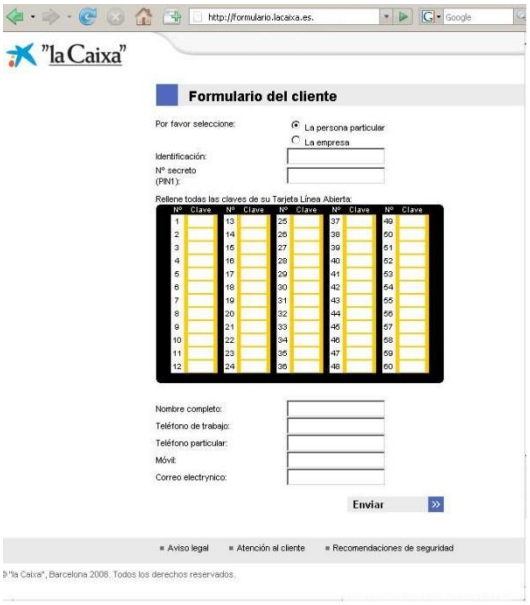


Figura 3.1.8: Un exemple d'una pàgina amb formulari clonada de La Caixa.

## Pharming

En aquest cas el *phisher ataca* al servidor *DNS* de la víctima. Pot ser de manera local, modificant la *cache*, redirigint el servidor *DNS* de la víctima (Figura 3.1.9), com un atac directe de servei *DDOS*, modificant els paràmetres del servidor *DNS*. En qualsevol dels dos casos, al navegar per internet la víctima serà redirigida als dominis web de l'atacant.

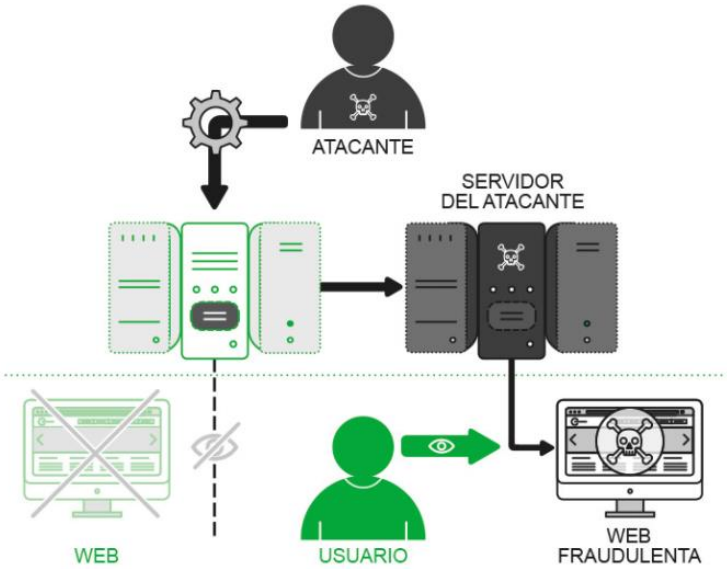


Figura 3.1.9: Funcionament pharming de canvi de servidor DNS.

**Vishing**

Es tracta de fer estafes mitjançant trucades de telèfon. Recentment, ha anat disminuint la quantitat d'estafes d'aquest mitjà. Poc a poc ha evolucionat *smishing* o *SPIM* phishing. Però segueix sent un medi utilitzat en certs camps i molts països en vies de desenvolupament.

**Smishing**

És una variant del *vishing* però en aquest cas es propaga per SMS. Existeixen diversos mètodes per la recaptació: demanar entrar a un enllaç, trucar a un número de telèfon, etc.

**SPIM**

*SPIM* és la forma evolutiva de *vishing* i el *smishing*. S'utilitza els sistemes de missatgeria directe dels telèfons o xarxes socials, normalment fan servir sistemes de missatgeria automatitzada. (Figura 3.1.10)


**Figura 3.1.10: Exemple d'un intent de SPIM phishing amb WhatsApp.**

## 3.1.7 Etapes del *phishing*

La tècnica *phishing* és pot separar en 5 etapes diferenciades (ECS - European Cyber Security Organisation, s.f.):

- Recol·lecció d'informació de les víctimes
    - En aquesta etapa s'utilitzen medis externs per obtenir informació de les víctimes. L'atacant aprofitarà aquesta informació per adaptar l'atac amb tècniques de l'enginyeria social i així augmentar les probabilitats d'èxit.
- Implementació de la infraestructura
    - Aquesta etapa és coneguda com "*Building"* i tracta de construir tota la plataforma tecnològica que envolta l'atac. És una etapa bastant volàtil ja que s'ha de construir sota el precepte de no deixar rastre. Poder muntar i desmuntar fàcilment.
- Disseny i llançament del atac
    - Aquesta etapa és coneguda com "*Spoofing"* o *"Cloning"*. És la fase de disseny de l'atac. També inclou tota la fase de programació del atac.
- La captació de víctimes. "*Baiting*"
    - Aquesta etapa és el procés d' espera per a la captació de víctimes.
- La recol·lecció d'informació. "*Harvesting*"
    - Aquesta etapa és la que tracta de danyar o beneficiar-se tot el possible de la víctima.

## 3.2 Situació actual del Phishing

En aquest punt farem una mirada amb profunditat del "*State of the Phish*", la situació actual del Phishing[6].

### 3.2.1 Balanç de l'any 2020

Durant l'any 2020 s'han registrat grans volums d'atacs phishing dirigits a una gran varietat d'empreses. Més del 75 % de les organitzacions asseguren haver enfrontat atacs de phishing amb diferents metodologies. El mètode més usual registrat és el Email phishing dirigit a múltiples persones.

Però s'ha de tenir en compte que tot i que el més detectat és l'email phishing, el que més afecta a les empreses és el Spear phishing - Whaling o BCE[7] ja que són els més difícils de

[6] State of the phish estat del phishing actual segons informes anuals de Proofpoint i Crackwatch.
[7] BEC o Whaling. Business email compromise attack. Conegut com un atac dirigit a alts càrrecs d'empreses

detectar, classificar i els que més danys produeixen i són els que van dirigits a càrrecs o víctimes concretes.

En la Figura 3.2.1 i la Figura 3.2.2 podem observar el volum d'atacs identificats. Spear pishing - whaling i BCE.

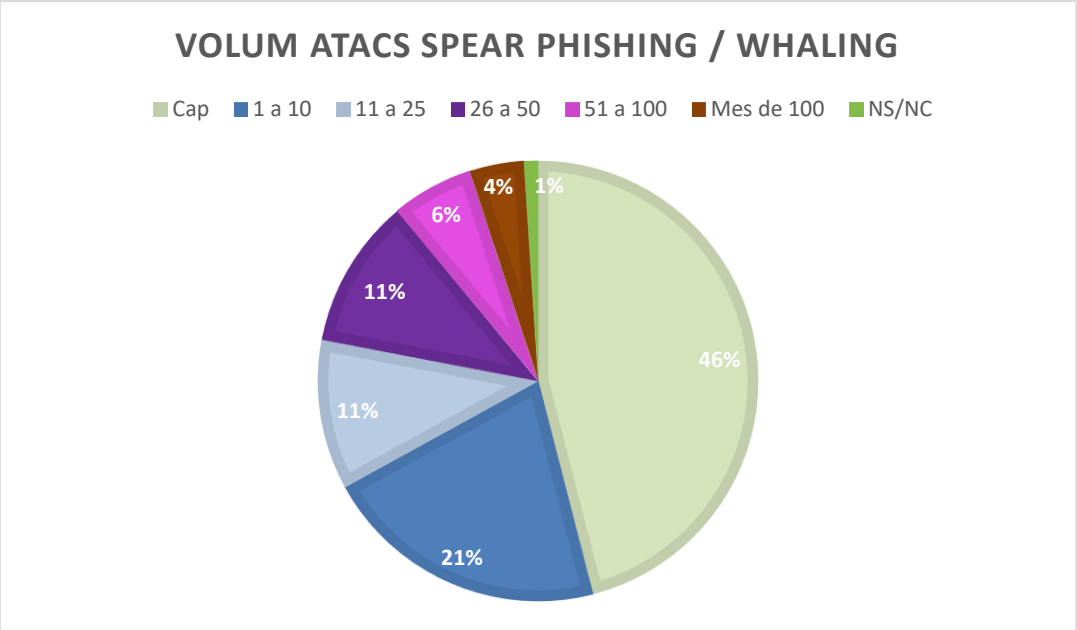


Figura 3.2.1: Proofpoint. "Geofenced Amazon Japan Credential Phishing Volumes Rival Emotet," Octubre 2020

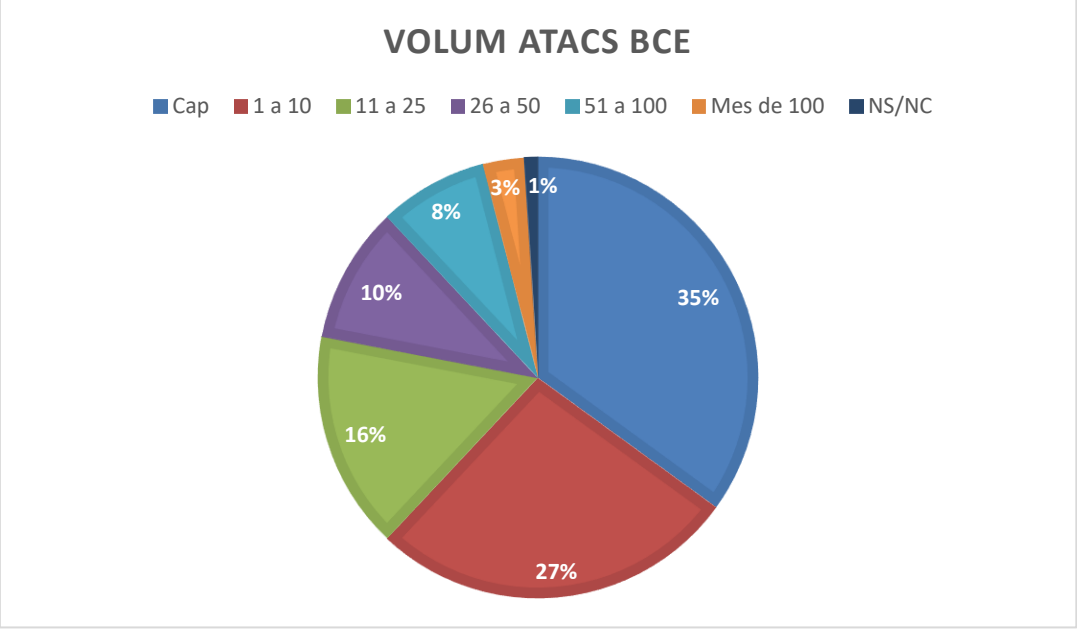


Figura 3.2.2: Proofpoint. "Geofenced Amazon Japan Credential Phishing Volumes Rival Emotet," Octubre 2020

Com es pot observar el 66% i el 65% de les empreses detecten algun format de phishing per Email.

També s'ha de fer menció als atacs no dirigits per Email com: xarxes socials, telèfon (smishing) o altres medis.

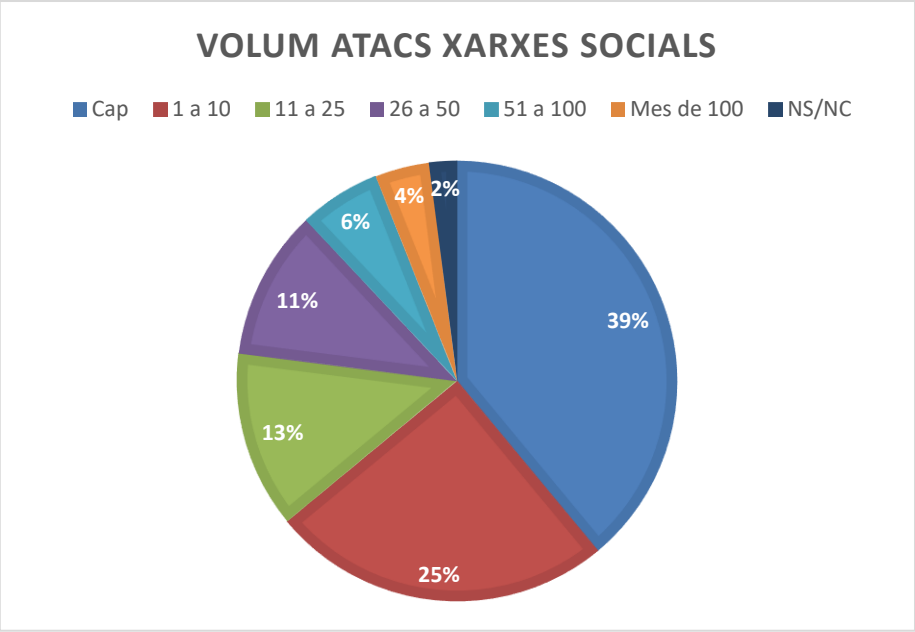


Figura 3.2.3: Proofpoint. "Geofenced Amazon Japan Credential Phishing Volumes Rival Emotet," Octubre 2020

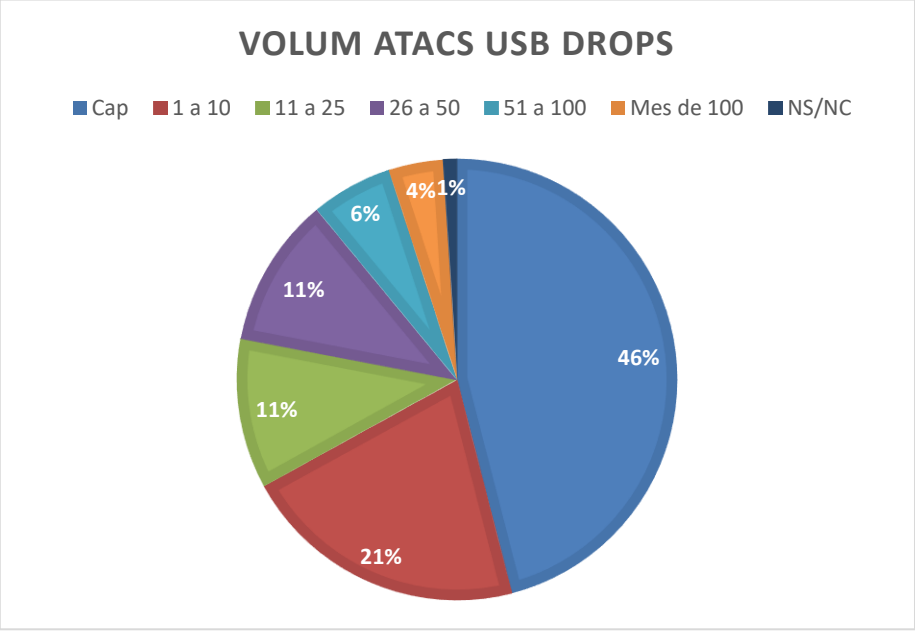


Figura 3.2.4: Proofpoint. "Geofenced Amazon Japan Credential Phishing Volumes Rival Emotet," Octubre 2020

Com es pot observar en aquests casos són menys registrats però són en gran mesura focus importants d'atacs.

S'ha de tenir en compte que aquestes dades no representen l' efectivitat dels atacs, sinó el seu volum, les dades d'efectivitat s'ha fet en el següent mostratge.

En la Figura 3.2.5 es mostren el percentatge d'efectivitat d'atac de tipus Ransomware[8]. Comparativa entre 2020 i 2019.

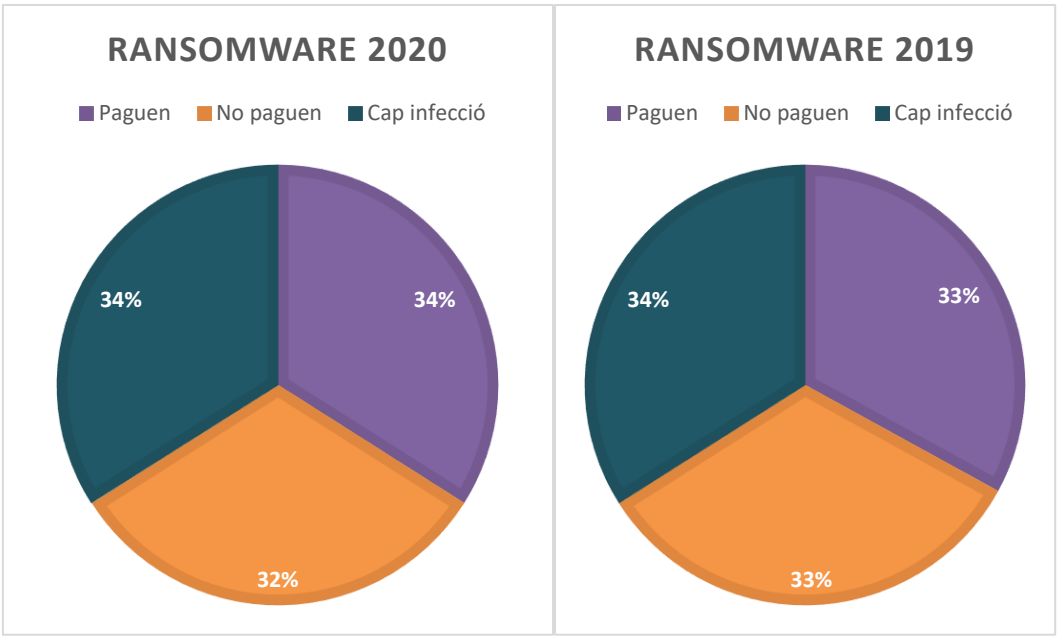


**Figura 3.2.5: Proofpoint State of the phish 2020.**

Es pot observar que el 2020 hi ha un augment discret del percentatge d'organitzacions que opten per pagar als segrestadors. Però és important recalcar que, tot i cooperar, molts cops no és una garantia de que retornin les dades segrestades.

[8] Ransomware. Un programa maliciós de segrest de dades amb l'objectiu d'extorsionar a la víctima.

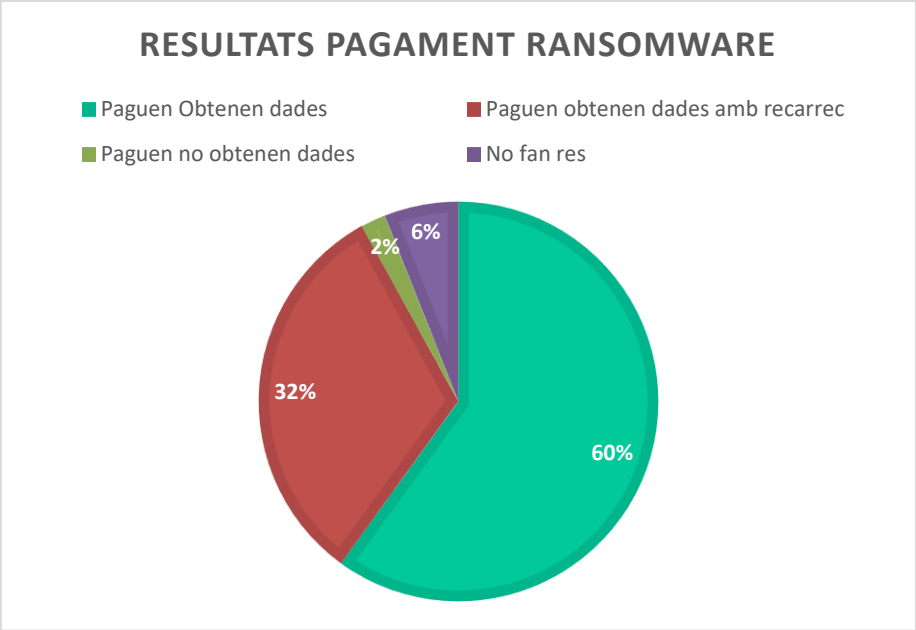


**Figura 3.2.6: Proofpoint State of the phish 2020.**

En la Figura 3.2.6 es pot identificar que dels resultats obtinguts d'organitzacions afectats per atac de Ransomware el 2020. Un 32 % de les organitzacions requerien de pagaments addicionals en que la gran majoria incrementada fins a un 320 % dels costos inicials exigits.

### 3.2.2 Perfil de l'atacant

L'atacant anomenat normalment *hacker* o *phisher*. És aquell actor informàtic que té com objectiu trobar vulnerabilitat als sistemes informàtics o de telecomunicacions. S'ha de diferenciar que *hacker* no és sinònim de ciberdelinqüent. A diferència del *hacker* el ciberdelinqüent té com a objectiu obtenir un benefici de qualsevol tipus d'actiu obtingut amb aquestes vulnerabilitats al contrari que un *hacker* que no busca aprofitar-se.

La classificació d'atacants:

| Classificació dels atacants - *Thread Actors* | | | |
|---|---|---|---|
| Categoria | Denominació | Coneixements Tècnics | Quantitat de recursos |
| Aficionat | *Script Kiddies* | Baixos | Molt baixos |
| Activistes | *Hacktivists* | Mig | Baixos |
| Cibercriminal | *Financial Gain – Phisher* | Mig o Alts | Baixos - Mig |
| Ciber-organitzacions | *Ciber organizations* | Alts | Mig |
| Financer i Polític | *Trade Secrets and Global Politic* | Alts o Molt Alts | Molt Alts |
| Nacions-Estats | *States – cyberwar* | Molt Alts | Molt Alts |

**Taula 3.2.1: Llista tipus d'amenaces ciberseguretat - Cisco CCNA Cyberops Course**

La classificació segons origen:

En la Figura 3.2.7 es pot observar els primers deu països emissors de correu spam. Podem observar que les principals emissores són efectivament superpotències mundials, països amb economies emergents o en situació de setge o guerra. Això té relació amb el poder adquisitiu, poder polític i situació social de cada país.

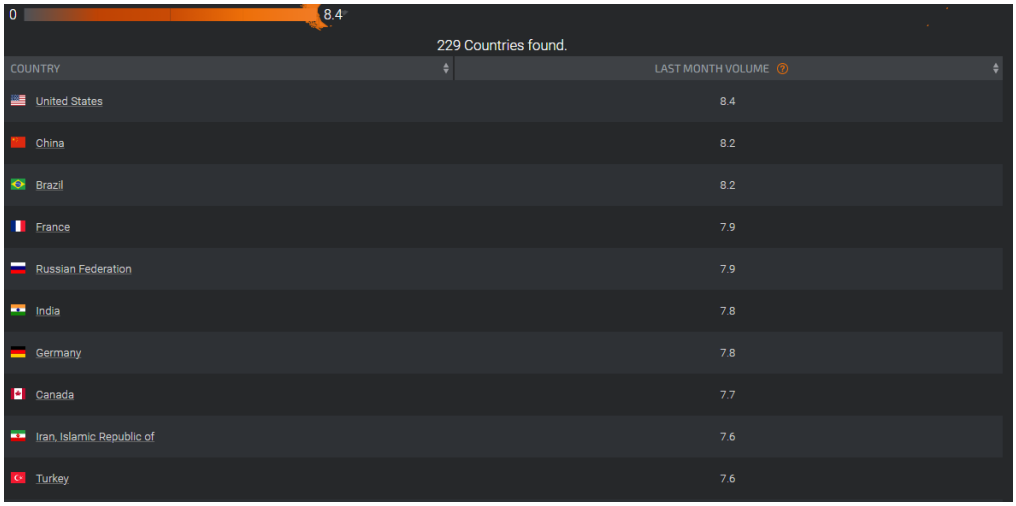


**Figura 3.2.7: Els deu primers països que envien spam i mètrica del volum. (Talos Intelligence Cyber Attack Map, 2021)**

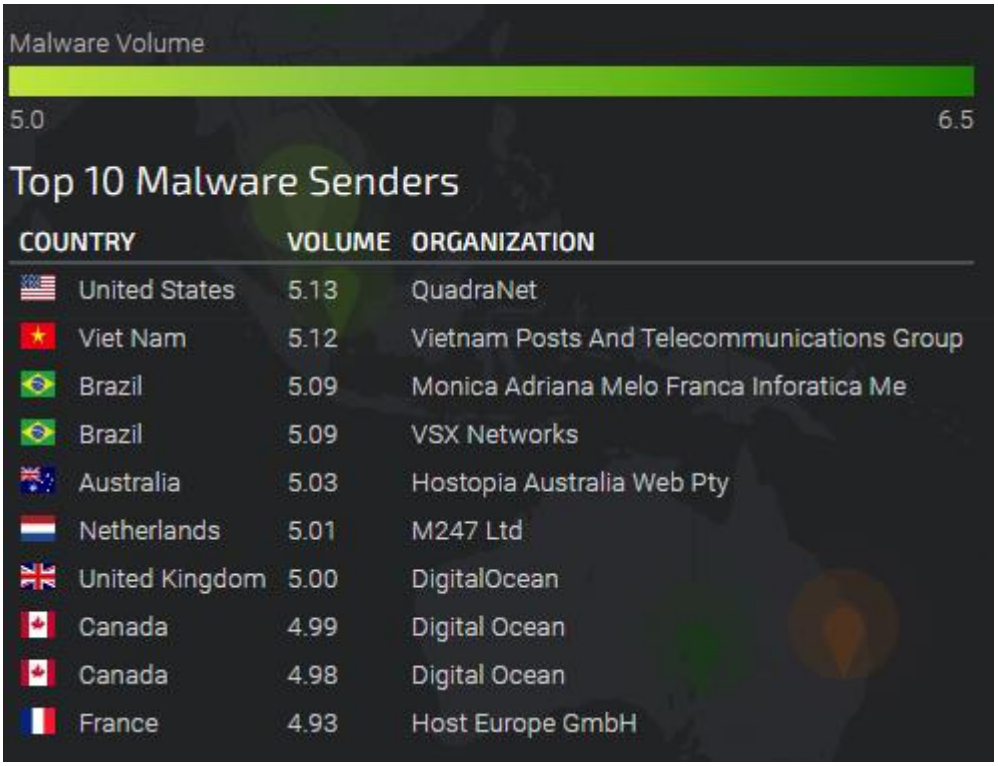


**Figura 3.2.8: Els deu primers països que envien malware i mètrica del volum. (Talos Intelligence Cyber Attack Map, 2021)**

### 3.2.3 Divisió per temàtica

En el sector del phishing existeix diferents temàtiques i tipologies d'atac. En la Figura 3.2.9 es pot observar el tipus de phishing més emprat. Les dades són realitzades via enviaments de prova controlat a entitats amb un resultat de 60 milions d'entrades.

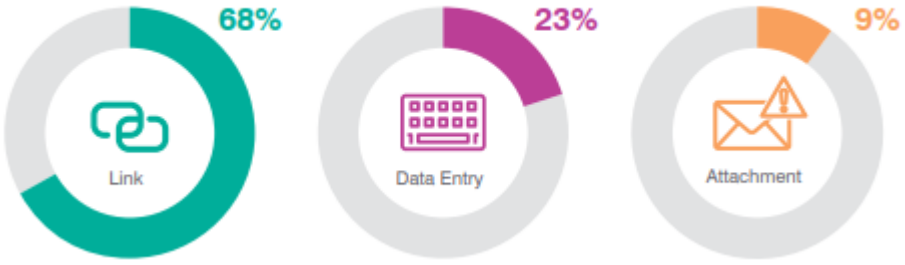


**Figura 3.2.9: Proofpoint State of the phish 2020. Frequencia d'ús.**

De seixanta milions de tests de phishing enviats a organitzacions l'any 2020. El 68 per cent dels atacs de tipus enllaç (url phishing), el 23 per cent d'entrada de dades basat en injecció de contingut (scripting) i el 9 per cent basat en adjunts van ser efectius (malware).

L'ús de l'atac tipus "link", beneficia a l'atacant per la facilitat d'emmascarar l'enllaç maliciós de la vista de l'usuari, normalment amagat dins d'elements: imatges, capçaleres, etc.

Podem observar que és necessari donar prioritat i coneixement als usuaris de que la gran majoria de vulnerabilitats apareixen de donar clic a elements, imatges enllaçades, capçaleres, enllaços afegits a text, per esmenar alguns.

Per sobre de tot el 2020, s'ha incrementat l'ús de serveis legítims per atacar via phishing com: Office 365, serveis de missatgeria, serveis de compartició d'arxius, serveis de compartició de contingut i xarxes socials.

La llista següent mostra alguns exemples de diferents temàtiques d'atacs documentats durant el 2020:

1. Oferta de subscripció a serveis de Streaming.

2. Campanyes de màrqueting falsificats.

3. Atacs de seguretat a xarxes socials.

4. Recollida o entrega de paquets.

5. Ofertes i campanyes en relació al Sars-Cov-2.[9]

6. Serveis d'informació i seguretat per a Sars-Cov-2.

7. Regularització de treball per Sars-Cov-2.

8. Office 365 recuperació de compta.

9. Alertes de connexió remota o inhabilitació del compte de OneDrive.

10. Alertes de missatgeria.

Podem observar que en el 2020 s'ha focalitzat en gran part al Coronavirus. Aquesta temàtica és adient perquè sigui aprofitada per criminals, ja que la desinformació, l'interès de les

[9] Sars-cov-2 més conegut com Covid-19 és una malaltia infecciosa que es va originar a la xina i va ésser responsable de la pandèmia global del 2019.

víctimes i situació de confinament facilita que les víctimes no puguin identificar prematurament l'atac.

### 3.2.4 Divisió geogràfica

Durant l'any 2020 s'han registrat diferents orígens de malware i phishing. En el cas de cinc països amb més origen d'atacs phishing la gran majoria han orientat els seus atacs amb temàtica Coronavirus o al sector mèdic-governamental.

| ACTOR | Tema COVID-19 | Orientat al sector mèdic | Orientat al sector governamental |
|---|---|---|---|
| Nord Korea | x | x | |
| Vietnam | x | | x |
| Iran | | x | x |
| Russia | | x | |
| Xina | x | | x |

Taula 3.2.2: CrowdStrike – Global Threat Report.

En la Taula 3.2.2 podem observar que més de la mitat han especificat els seus atacs amb temàtica del coronavirus, al igual que el sector mèdic.

En altres casos, s'han identificats atacs phishing de malware Ransomware. En aquest cas podem observar en la Figura 3.2.10 es pot observar la relació entre Estats Units i Espanya del percentatge de víctimes que finalment accepten cooperar i pagar.

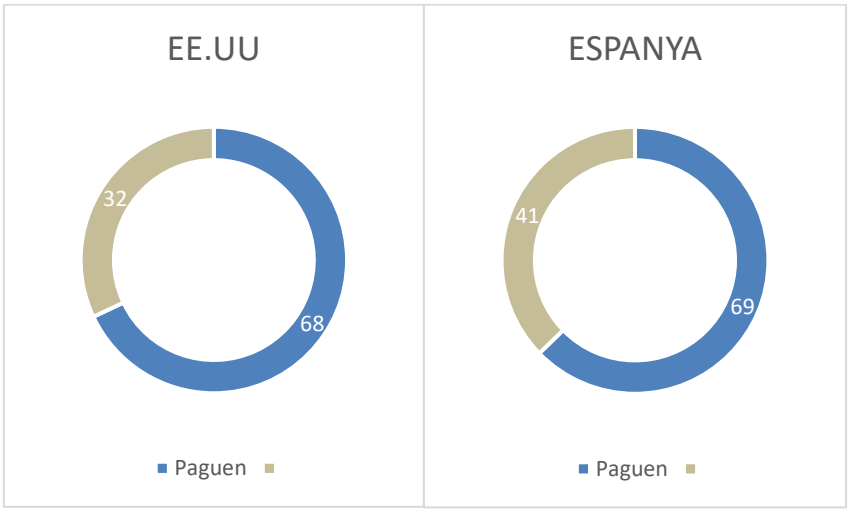


Figura 3.2.10: Proofpoint State of the phish 2020.

### 3.2.5 Divisió per sector

S'ha de destacar que a nivell organitzatiu quins són els sectors més vulnerables d'atacs. S'han registrat que els sectors amb més incidència són:

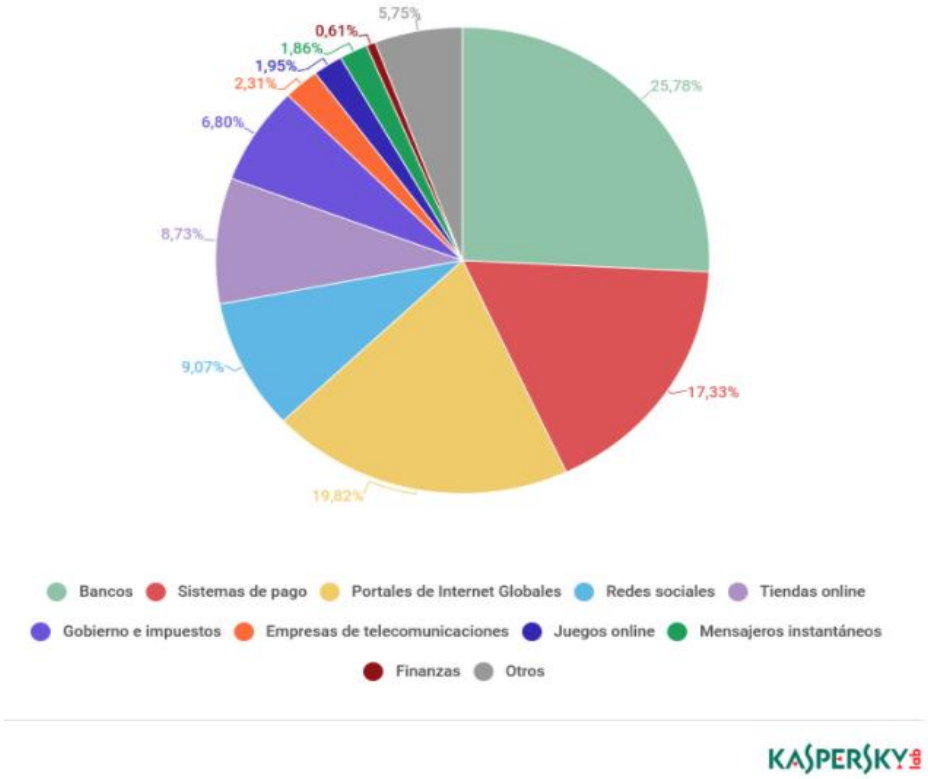


**Figura 3.2.11: Diagrama de sectors dels sectors més atacats per phishing 2019T1.**

La gran majoria són serveis de pagament, portals de compra, portals d'informació de banca i banca. En la Taula 3.2.3 podem observar quins són els sectors amb més incidència i la probabilitat de que els phishing siguin efectius.

**Average Failure Rate, Reporting Rate and Resilience Factor by Industry**

| Industry | Reporting Rate | Failure Rate | Resilience Factor |
|---|---|---|---|
| Financial Services | 20% | 11% | 1.8 |
| Energy/Utilities | 18% | 11% | 1.6 |
| Insurance | 17% | 10% | 1.7 |
| Legal | 17% | 8% | 2.1 |
| Engineering | 16% | 16% | 1.0 |
| Automotive | 15% | 8% | 1.9 |
| Business Services | 14% | 11% | 1.3 |
| Technology | 13% | 12% | 1.1 |
| Government | 13% | 10% | 1.3 |
| Mining | 13% | 13% | 1.0 |
| Food & Beverage | 11% | 11% | 1.0 |
| Manufacturing | 10% | 10% | 1.0 |
| Healthcare | 10% | 10% | 1.0 |
| Entertainment/Media | 10% | 9% | 1.1 |
| Transportation | 10% | 12% | –1.2 |
| Telecommunications | 9% | 14% | –1.6 |
| Construction | 9% | 11% | –1.2 |
| Retail | 9% | 13% | –1.4 |
| Education | 6% | 12% | –2.0 |
| Hospitality/Leisure | 5% | 10% | –2.0 |

**Taula 3.2.3: Proofpoint State of the phish 2020. Test phishing security test failed.**

Però dins de cada grup quins són els departaments on més efectivitat existeix. En la Figura 3.2.12 podem observar quins són els departaments amb més incidència i la probabilitat de que els atacs phishing siguin efectius.

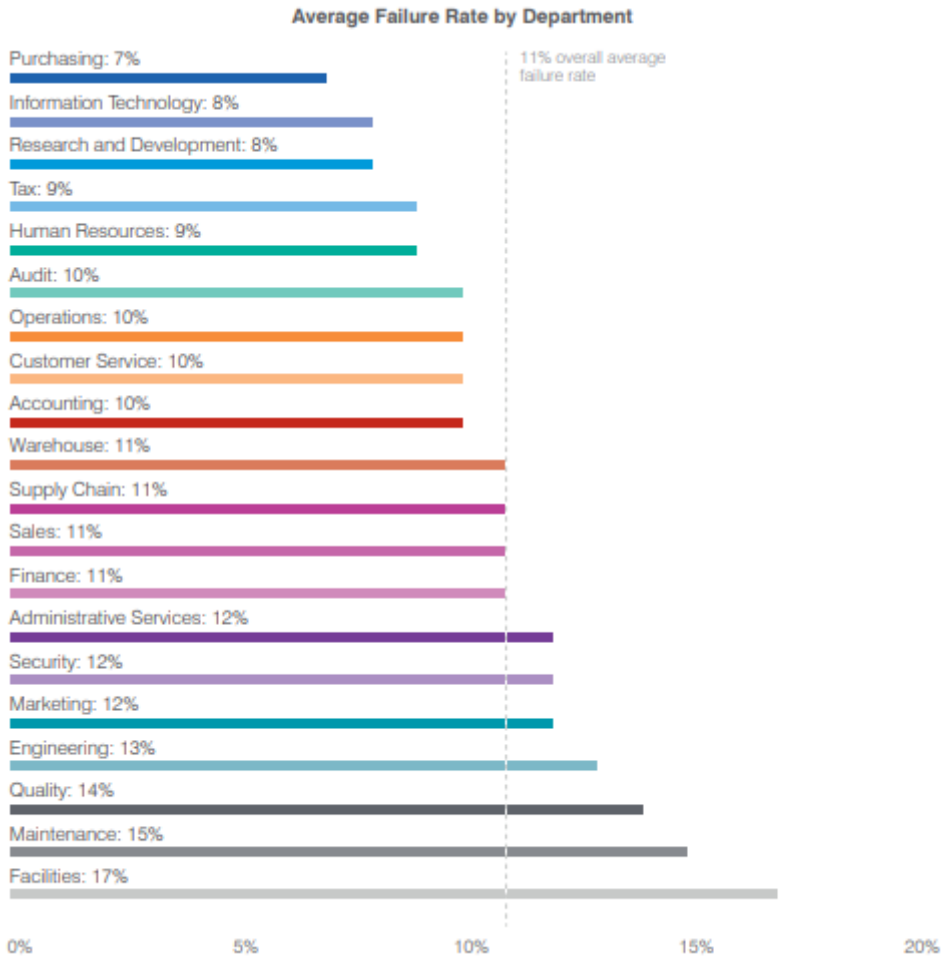


**Figura 3.2.12: Proofpoint State of the phish 2020. Test phishing security test failed by department.**

# 4. Bones pràctiques

## 4.1 Llista de bones pràctiques contra el phishing

En el món de la informàtica no existeix la seguretat permanent ni amb cent per de cent d'efectivitat, per tant, és important ser previngut i conèixer mètodes d'identificació. En aquest cas posem en pràctica deu consells per a la detecció prematura de *phishing.* (INCIBE - Kit de Concienciación)

1. Mirar abans de fer clic

   Ens ensenyen que abans de creuar el carrer hem de mirar als dos costats. El mateix amb els enllaços web. Abans de donar clic als enllaços mirem que és i qui els envia.
2. Actualitzar

   Utilitza software amb les versions més actualitzades. Els *phishers* aprofiten errors de versions anteriors amb errors per aprofitar les vulnerabilitats.
3. No utilitzar una contrasenya per tot

   Una contrasenya per a cada servei, comprova que no tinguis les credencials filtrades, no utilitzis una per tot. Segueix els consells de cada plataforma i no donis a ningú mai les credencials.
4. No es coneix, no es comparteix

   Si no coneixes al remitent o la pàgina no és familiar, no comparteixis ninguna informació.
5. No creure tot el que es veu

   No tot el que es veus és veritat, els *phishers* utilitzen totes les eines possibles per falsejar identitats, pàgines webs o firmes electròniques.
6. Vigilar els adjunts

   Els adjunts són portes d'entrada per al software maliciós.
7. En cas de dubte no seguir

   Els *phishers* aprofitaran del desconeixement i de la precipitació. En cas de dubte no seguir.
8. Preguntar als experts

   Pregunta als experts o busca informació abans de clicar. Els experts tenen eines de detecció i procediments.

9. Avisar tothom.

   Informa als experts i a les persones del teu voltant, si avises es poden evitar futurs problemes.

10. Utilitza eines de seguretat.

    Existeixen moltes eines de detecció i prevenció del *phishing.* Firmes digitals, certificats electrònics, software anti-virus, firewalls, etc.

# 5. Anàlisi de referents

## 5.1 Referents dins del sector

Dins del mercat de la ciberseguretat és difícil definir un grup d'empreses punteres del sector. Cada any la ciberseguretat incrementa la demanda d'experts en ciberseguretat, un increment que s'estima que es requeriran de 29.000 experts en ciberseguretat en els pròxims 3 anys només a Espanya i als Estats Units es requeriran de 360.000 experts.

Els referents dins del sector no sempre són els mes coneguts dins del mercat del IT. Ja que gran quantitat d'aquestes empreses generen productes desconeguts pel consumidor mig.

A continuació hi ha una llista d'empreses amb més repercussió dins del mercat de la ciberseguretat:

1. McAffee: (Ciberseguretat General)

2. Fortinet: (Ciberdefensa)

3. Blackberry Intelligence and Predictive Security: (IOT)

4. Dolbuck: (Auditoría)

5. Sophos: (Business Security)

6. TrendMicro: (Empreses i PIMES)

7. Rapid7: (Xarxes i servidors)

8. AT&T Cybersecurity (AlienVault): (Telefonia)

9. Electronic ID: (Governamental, processos electoral)

11. Blueliv: (Banca i financeres)

10. ElevenPaths Telefónica: (Ciberseguretat General)

## 5.2 Tecnologies phishing

***Phish kits***

S'anomena *phish kit* o *phishing kits* tota aquella col·lecció d'eines de software que permet a amb bastanta facilitat i sense moltes habilitats tècniques implementar un *exploit*[10] de *phishing.*

Existeixen moltes compilacions d'aquestes eines amb un ventall d'objectius i de implementacions.

En aquest cas ens centrarem en el funcionament d'un *phish kit* anomenat PhishX. És una eina de *phishing* dirigit a fer *spear phishing*. Aquesta eina té com objectiu fer *spoofing* de xarxes socials.

Envia un correu electrònic fals de la xarxa social. I fa una petició per un problema de seguretat i demana canvi de contrasenya mitjançant un enllaç fals. Posteriorment envia el registre d'entrada que ha fet la víctima amb contrasenya actual i la nova contrasenya al servidor entrant del *phisher*.

Podem trobar tota la documentació al enllaç a GitHub. (Usuari kratos64, 2018)

**Prova de funcionament *spear phishing* amb *PhishX*.**

La prova realitzada és un exemple del proveïdor que s'ha executat en un servidor Kali-linux (Usuari kratos64, 2018), dependències del software:

- Python 2.7 o posterior.

- Servei SMTP en aquest cas s'ha utilitzat un smtp.mailtrap.io

- Servidor WEB en aquest cas és un Apache 2.4.

Comandes d'instal·lació del software.

```
$ git clone git@urlphishkit.git
$ cd PhishX
```

[10] Exploit és una paraula d'origen anglès que significa aprofitar. Normalment són parts de software, comandes o accions amb la fi d'aprofitar vulnerabilitats de seguretat de sistemes d'informació.

```
$ chmod +x installer.sh
$ bash installer.sh
$ python3 PhishX.py
```

En la Figura 5.2.1 es pot observar la pantalla principal al executar el *PhisX.py*.

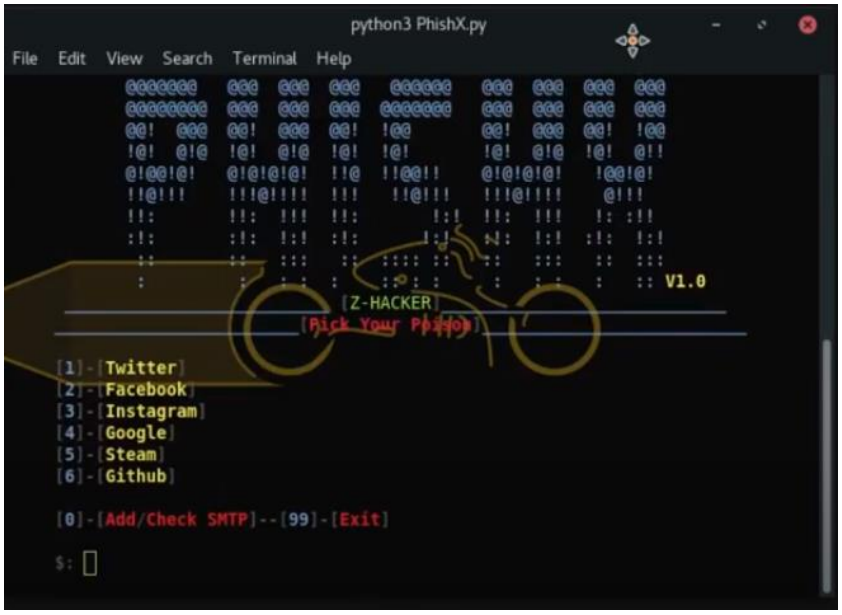


**Figura 5.2.1: Captura de pantalla de la pantalla principal del programa PhishX.**

Seguidament s'introdueixen les dades del servidor SMTP i l'usuari que rep els correus electrònics de les víctimes. (Figura 5.2.2)

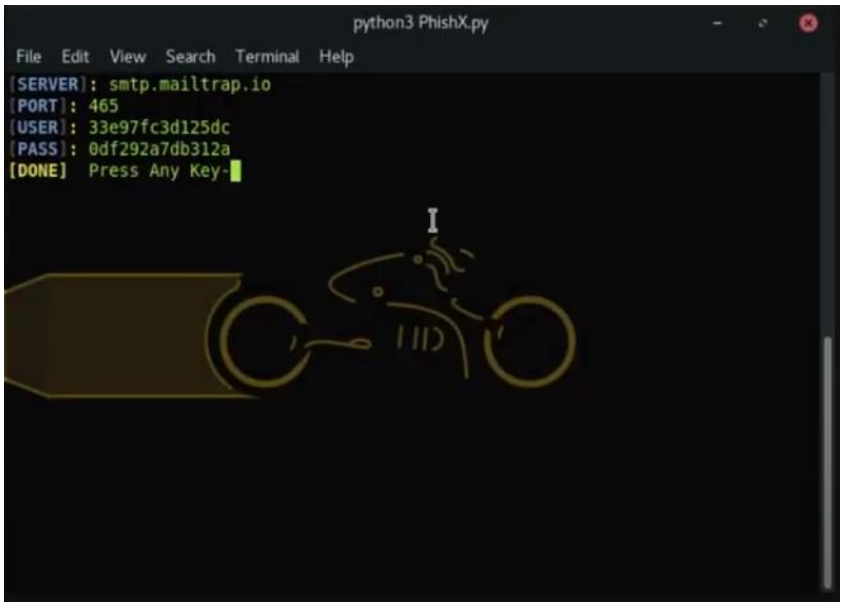


**Figura 5.2.2: Captura de pantalla de exemple d'introducció de paràmetres SMTP.**

Després d'introduir les dades del correu electrònic ja podem realitzar el atac *phishing.* En aquest cas escollim fer un atac a un usuari de Facebook, opció 2. (Figura 5.2.3)

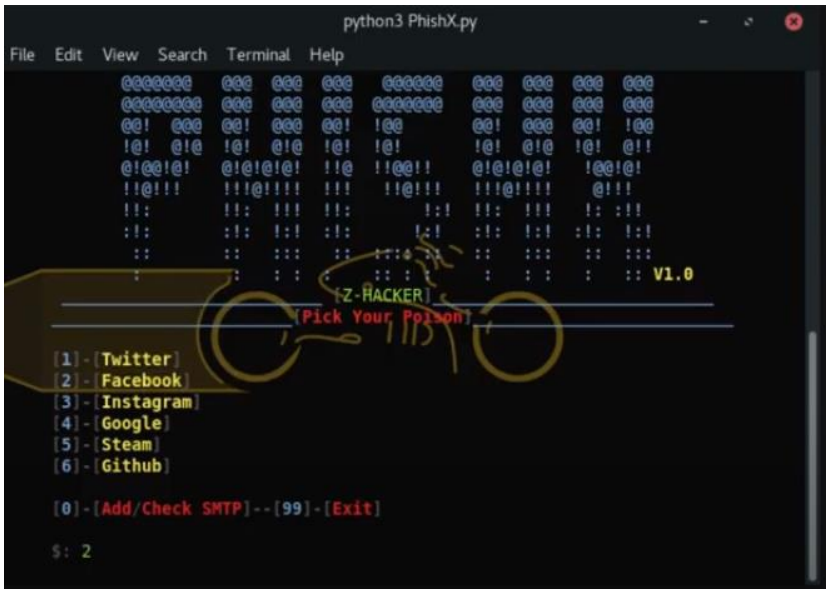


**Figura 5.2.3: Captura de pantalla de selecció de plataforma escollida.**

S'escull el destinatari de l'atac en aquest cas és un usuari de prova. Però la informació és fàcil d'aconseguir només accedint a la pàgina, ja que, la gran majoria de la informació és d'accés públic. El indispensable per utilitzar aquest atac és el identificador d'usuari (públic), el nom d'usuari (públic) i el correu electrònic (públic). (Figura 5.2.4)

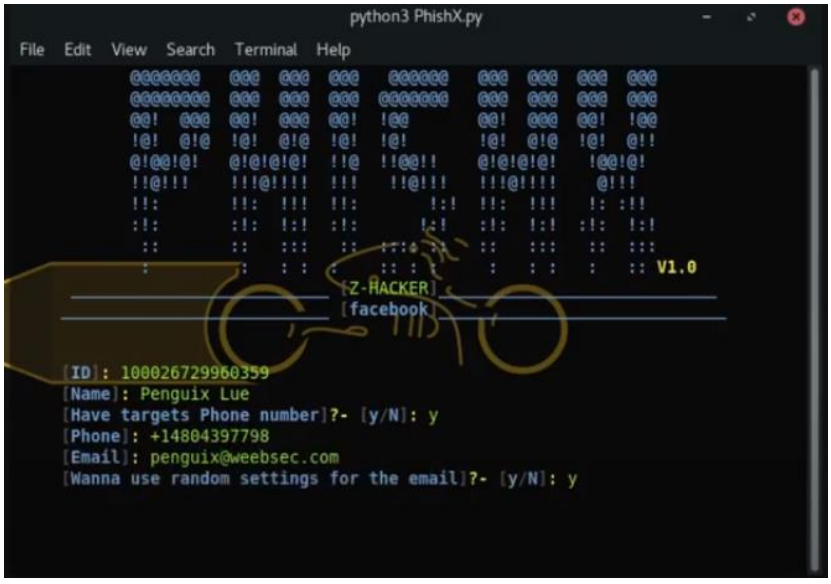


**Figura 5.2.4: Captura de pantalla de introducció de informació. de la víctima.**

A posteriori ja només s'ha d'esperar a la resposta de la víctima. Aquesta rep un correu electrònic. (Figura 5.2.5)

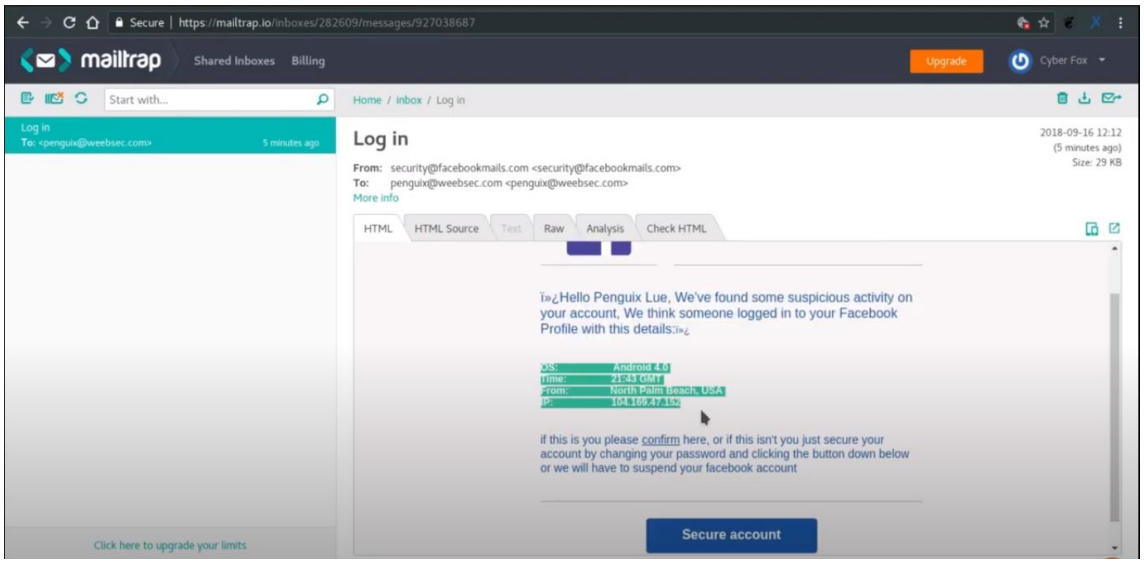


Figura 5.2.5: Captura de pantalla del correu rebut per la víctima.

La víctima al donar clic a "secure account" obre un enllaç al servidor web de l'atacant amb una petició de canvi de contrasenya. (Figura 5.2.6, Figura 5.2.7, Figura 5.2.8)

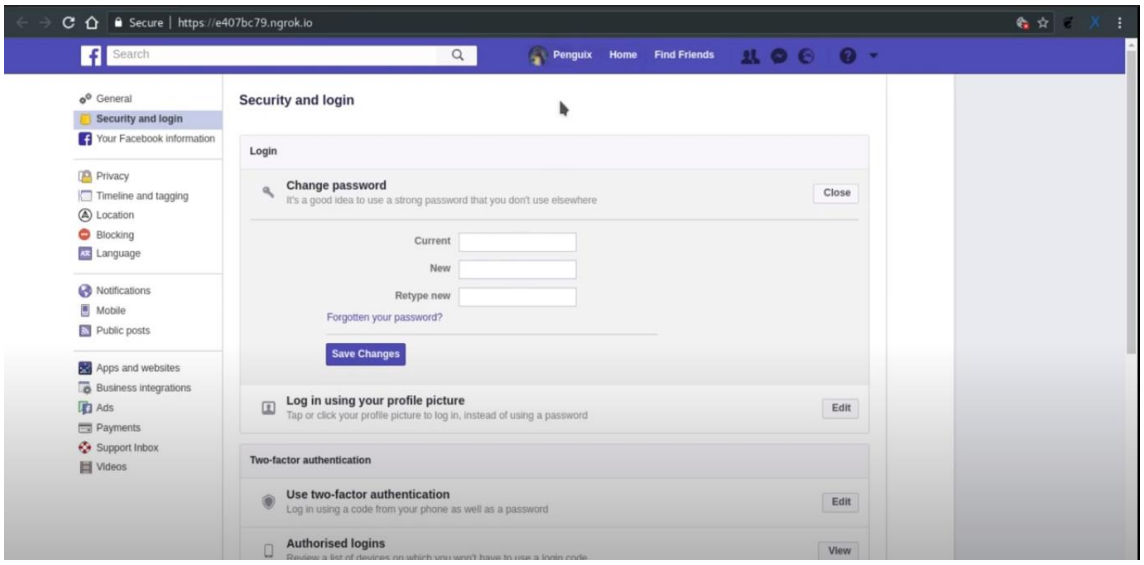


Figura 5.2.6: Captura de pantalla del enllaç de pàgina spoofing.

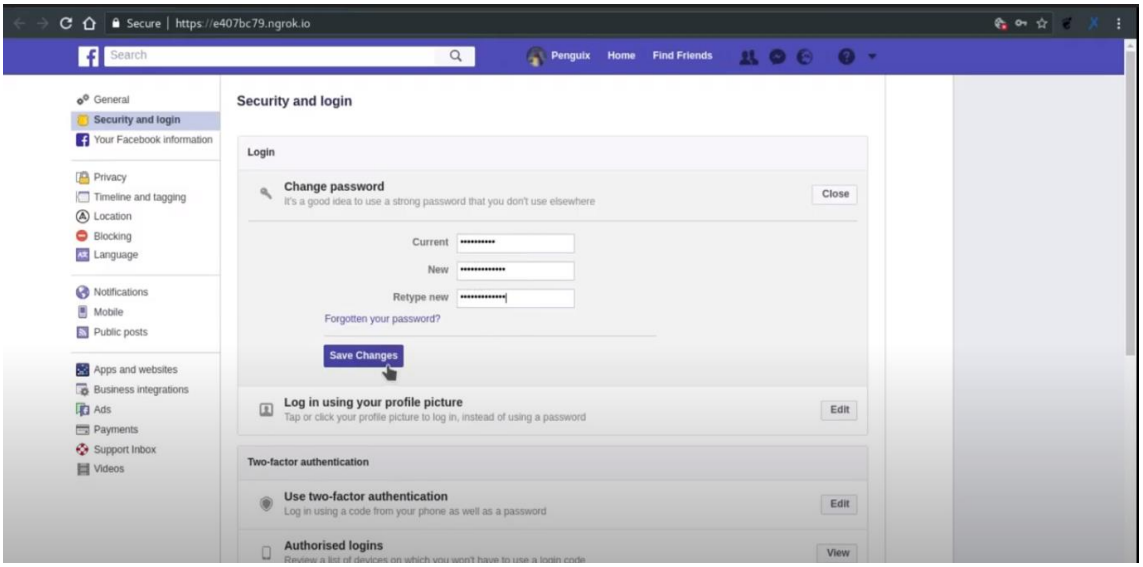


**Figura 5.2.7: Captura de pantalla enllaç de segona pàgina spoofing.**

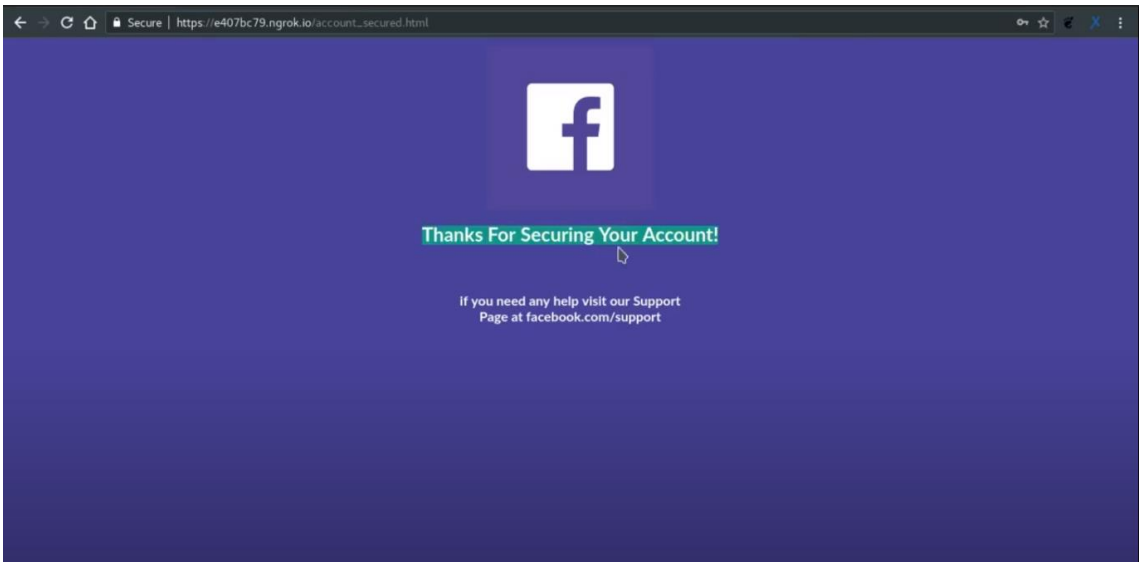


**Figura 5.2.8: Captura de pantalla del resultat spoofing.**

Finalment el *phisher* rep la informació al servidor amb les dades d'origen i l'entrada de dades de la víctima. (Figura 5.2.9)

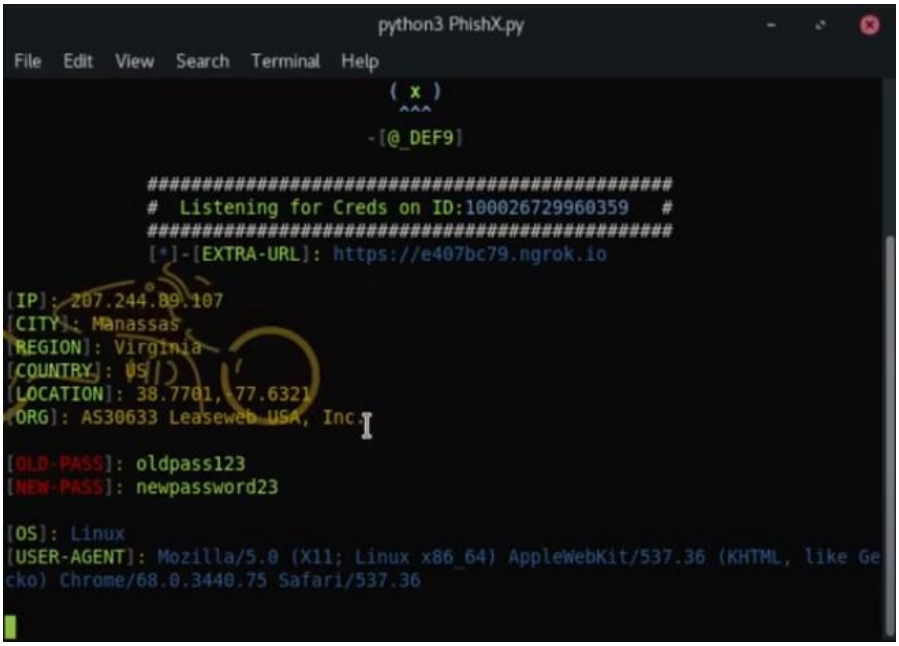


**Figura 5.2.9: Captura de la resposta rebuda amb la informació de la víctima**

Amb aquest exemple podem observar la facilitat d'implementar i llençar un atac tipus *phishing*. Podem observar que el *phisher* pot obtenir les credencials de l'usuari amb pocs recursos i ràpidament.

## 5.3 Tecnologies de detecció

Els casos de *phishing* web poden ser detectats de diferents maneres en aquest cas analitzarem eines preexistents d'anàlisi de contingut web.

Sistemes OSINT:

OSINT "Open Source Intelligence" és una eina de detecció de pàgines web *phishing* obert, és a dir, utilitzen fonts i llistes categoritzades per la comunitat. Utilitzen eines de reconeixement de patrons usualment utilitzats en el *phishing*. (INCIBE - OSINT, 2014)


Figura 5.3.1: Fases de reconeixement OSINT

Problemes dels sistemes OSINT:

- Massa informació:
    - La quantitat de informació pública genera un problema de processament i selecció de les fonts. Això provoca que el procés de classificació sigui lent i requereixi una gran quantitat de recursos.
- Fiabilitat de les fonts:
    - Les col·leccions obertes de dades es important valorar les fonts. En els casos de mal ús o del origen no contrastats pot generar resultat erronis i desinformació.

Plataformes que utilitzen sistemes OSINT:

- Phishtank. (Phishtank, s.f.)
- OpenPhish. (OpenPhish, s.f.)

Sistemes anàlisi IOCs:

Un sistema d'anàlisi web en IOCs "Indicators of Compromise" indicadors de compromís és una tecnologia estandarditzada que consisteix en definir les característiques tècniques de les amenaces.

L'objectiu és identificar els fitxers d'origen del atac, analitzar el contingut i mitjançant altres fitxers prèviament obtinguts realitzar un anàlisi de similitud. (INCIBE IOCs, s.f.)

Problemes dels sistemes d'anàlisi IOCs:

- Recol·lecció lenta:
    - Per tenir un sistema d'anàlisi IOC s'ha de tenir una llibreria de fitxers actualitzat. Això genera una gran quantitat de recursos que s'han d'anar processament periòdicament .
- Sistema amb gran demanda:
    - L'anàlisi comparatiu és un procés que pot requerir de molts recursos de processament.

Plataforma IOCs oberts:

- OpenIOC (OpenIOC, s.f.)
- IOC Bucket (IOC Bucket, s.f.)

# 6. Metodologia

## 6.1 Plantejament del projecte

El sistema està distribuït en dos blocs diferenciats.

El bloc servidor *Backend* el cercle de color blau i el bloc de pàgina web *Frontend* quadrat de color taronja. (Figura 6.1.1)

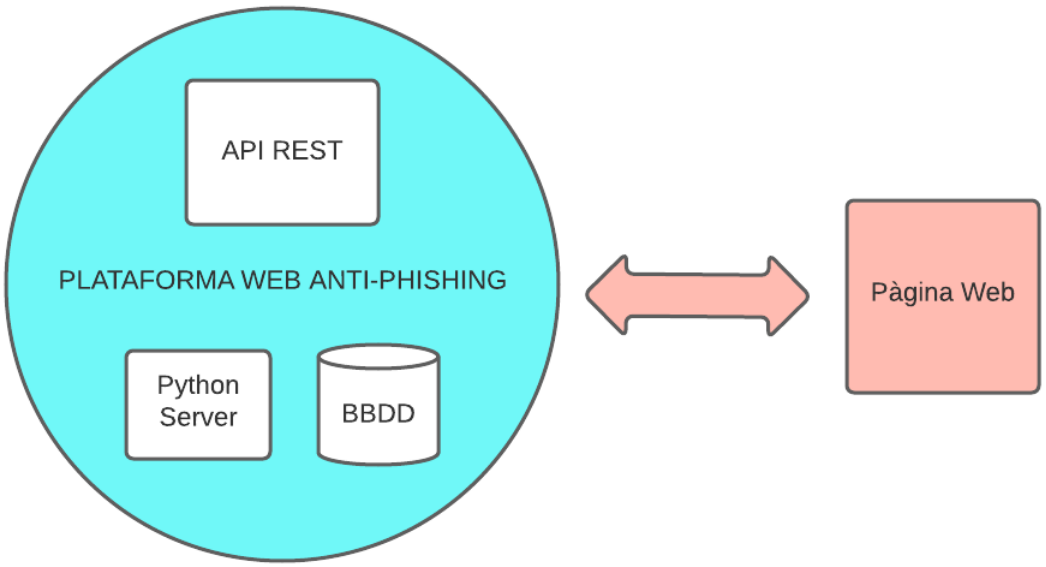


**Figura 6.1.1: Diagrama de blocs conceptual del sistema.**

.

El sistema està distribuït d'aquesta manera ja que el nucli del projecte es la plataforma web que serà l'encarregada de treballar les consultes, preparar i distribuir les dades.

## 6.2 Metodologia de desenvolupament

El desenvolupament s'ha realitzat mitjançant metodologia àgil SCRUM.

Cada implementació s'ha realitzat en iteracions de dues setmanes.

Cada "Sprint" o iteració inclou: planificació de la iteració, disseny, desenvolupament, implementació i finalment revisió.

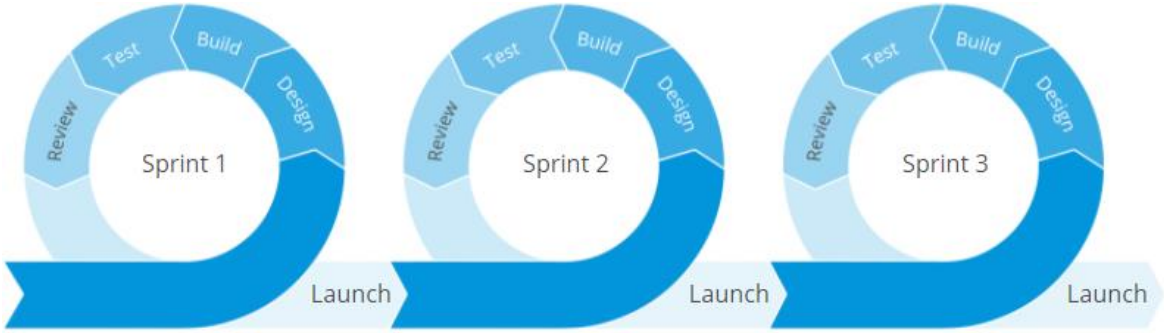


**Figura 6.2.1: Exemple de la metodologia Agile que s'ha emprat en el projecte.**

També s'ha seguit la metodologia TDD [11] tal i com recomana "Django developing directives[12]" per a la creació de model i dades.

## 6.3 Infraestructura

La infraestructura necessària del projecte. Tant de desenvolupament, com d'implementació i documentació són:

- Servidor web.
    - VPS M IONOS: 2vCores, 2GB RAM, 80 GB memòria
- Web hosting. Inclòs servei IONOS.
- Incorpori l'interpretador de *Python*.
- Bases de dades SQLite - *PostgreSQL*.

Mínim un ordinador de desenvolupament amb accés a internet amb els següents requeriments mínims:

- Processador: Intel i3 - 4xxx o superior / AMD Ryzen 3 2xxx o superior
- Memòria RAM: 8 GB
- Unitat de memòria: 500 GB
- Sistema operatiu: Windows 10, macOS Sierra o superior, Debian based (Ubuntu, Kali)

[11] TDD (Test-driven development) o Desenvolupament guiat per proves és una metodologia de desenvolupament on prioritza la creació de les proves (Tests) com a punt inicial de treball i a posteriori programar.
[12] Django development directives són una llista de bones pràctiques recomanades en la documentació pel desenvolupament d'aplicacions web en Django Python.

# 7. Desenvolupament

## 7.1 Anàlisi i definició de requeriments

Els requeriments dels projecte s'han dividit en dues parts un de l'anàlisi de tecnologies d'identificació del sector phishing i en generar una plataforma web que resolgui la problemàtica d'identificació de pàgines potencialment perilloses.

**Requeriments d'anàlisi:**

- Cronologia i evolució del sector del *phishing* informàtic.
- Estat actual del sector del *phishing* informàtic.
- Tècniques d'atacs tipo *phishing*.
- Metodologia dels atacs tipo *phishing.*
- Tecnologies tipo *phishing.*
- Metodologia *anti-phishing web* .
- Tecnologia *anti-phishing web*.
- Crear una llista de bones pràctiques contra el *phishing*.

**Requeriments de la plataforma web:**

- Identificació d'una URL *Phishing spoofing* falsedat de la pàgina web
- Mostrar al usuari una llista amb la mètrica de seguretat.
- Mostrar una llista de bones pràctiques contra aquestes tècniques per a l'usuari.

## 7.2 Casos d'ús del sistema

### CA_U.1. Cercar perillositat a l'aplicació

**Nom:** Cercar perillositat

**Descripció:** L'usuari ha de poder entrar un enllaç de domini web a la pàgina web.

**Actor:** Usuari web

**Pre-condicions:**

- L'usuari ha d'haver obert la pàgina web.

**Post-condicions:**

- L'usuari veu el resultat de la cerca de perillositat en una mètrica resultant.

**Flux normal d'execució:**

100. L'usuari introdueix al bloc de text l'enllaç web que vol cercar.

200. L'usuari prem cercar.

300. El sistema cerca la entrada del usuari.

400. El sistema mostra el resultat al usuari i mostra una llista de bones pràctiques..

**Flux alternatiu:**

400. En cas d'haver un error, mostra un missatge d'error al usuari.

**Diagrama:**

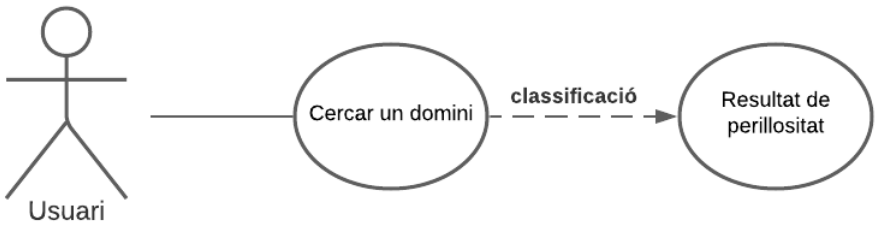


Figura 7.2.1: Diagrama de cas d'ús CA_U1

### CA_U.2. Mostrar al usuari una llista de bones pràctiques.

**Nom:** Mostrar llista de bones pràctiques

**Descripció:** L'usuari ha de poder cercar informació de bones pràctiques contra el *phishing*.

**Actor:** Usuari web

**Pre-condicions:**

- L'usuari ha d'haver obert la pàgina web.

**Post-condicions:**

- L'usuari veu informació de bones pràctiques contra el *phishing*.

**Flux normal d'execució:**

100. L'usuari prem el botó d'informació

200. El sistema mostra informació de bones pràctiques.

**Flux alternatiu:**

200. En cas d'haver un error, mostrar un missatge d'error al usuari.

**Diagrama:**

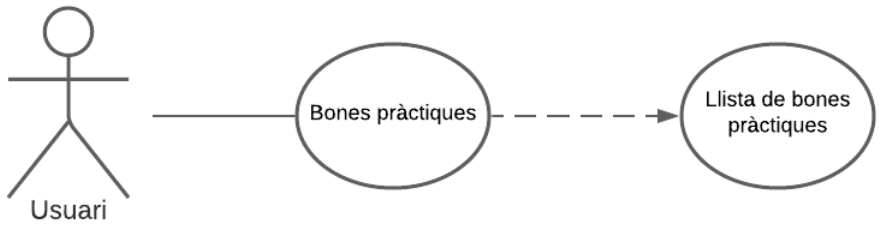


Figura 7.2.2: Diagrama de cas d'ús CA_U2

### CA_U.3. Obtenir resposta en format JSON.

**Nom:** Mostrar en un format JSON la informació de la pàgina introduïda.

**Descripció:** L' usuari ha de poder entrar un enllaç de domini web a la pàgina web i obtenir la informació en format JSON.

**Actor:** Usuari web

**Pre-condicions:**

- L' usuari ha d'haver obert la pàgina web.

**Post-condicions:**

- L' usuari veu informació de bones pràctiques contra el *phishing*.

**Flux normal d'execució:**

100. L' usuari introdueix al bloc de text l'enllaç web que vol cercar.

200. L' usuari prem cercar.

300. El sistema mostra una pantalla de processament.

400. El sistema mostra el resultat al usuari i mostra una llista de bones pràctiques.

500. El sistema guarda la cerca a la base de dades.

600. L' usuari prem el botó d'exportar a JSON.

700. El sistema converteix la informació en format JSON.

800. El sistema mostra la informació en format JSON.

**Flux alternatiu:**

400. En cas d'haver un error, mostrar un missatge d'error al usuari.

**Diagrama:**

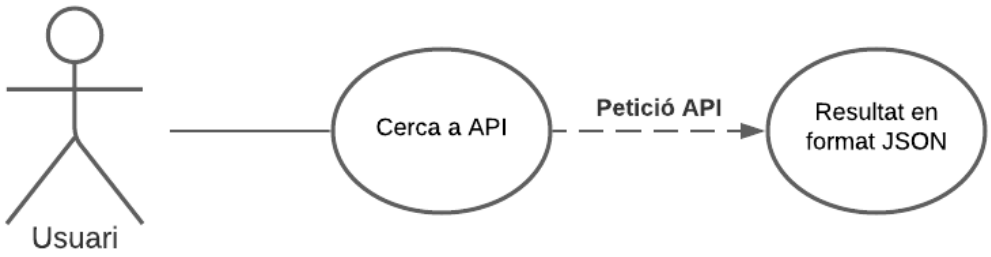


Figura 7.2.3: Diagrama de cas d'ús CA_U3

## 7.3 Disseny del software

El software s'ha decidit utilitzar el framework web de codi obert Django amb Python amb llicència BSD[13].

El software basat en Django té una arquitectura amb patró MVC (Model Vista Controlador) però amb una re definició anomenada MVT (Model Vista Template).

- Model: S'encarrega de fer la consulta a BD i de crear l'estructura dels objectes.
- Vista: En aquest cas Django té dues parts principals, url.py i views.py aquestes parts són les encarregades de fer de controlador al contrari que MVC.
- Template: El *template* és la part que s'envia de resposta a l'usuari, és a dir la Vista en MVC.

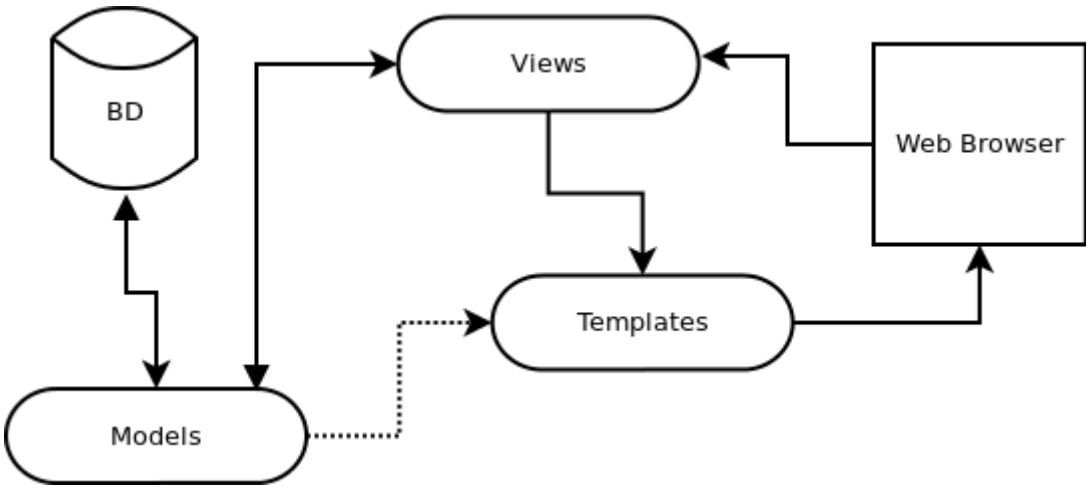


**Figura 7.3.1: Exemple de comunicació estandadr MVT Django.**

Django també implementa per defecte una implementació de model de dades amb desenvolupament TDD. Sempre és desenvolupa primer el test i a posteriori la implementació.

La seqüència d'implementació en MVT seria la següent:

tests.py → models.py →views.py → urls.py → templates/feature.html

L'estructura d'arxius en el projecte:

[13] *Berkeley Software Distribution:* És una llicència de software lliure permissiva.

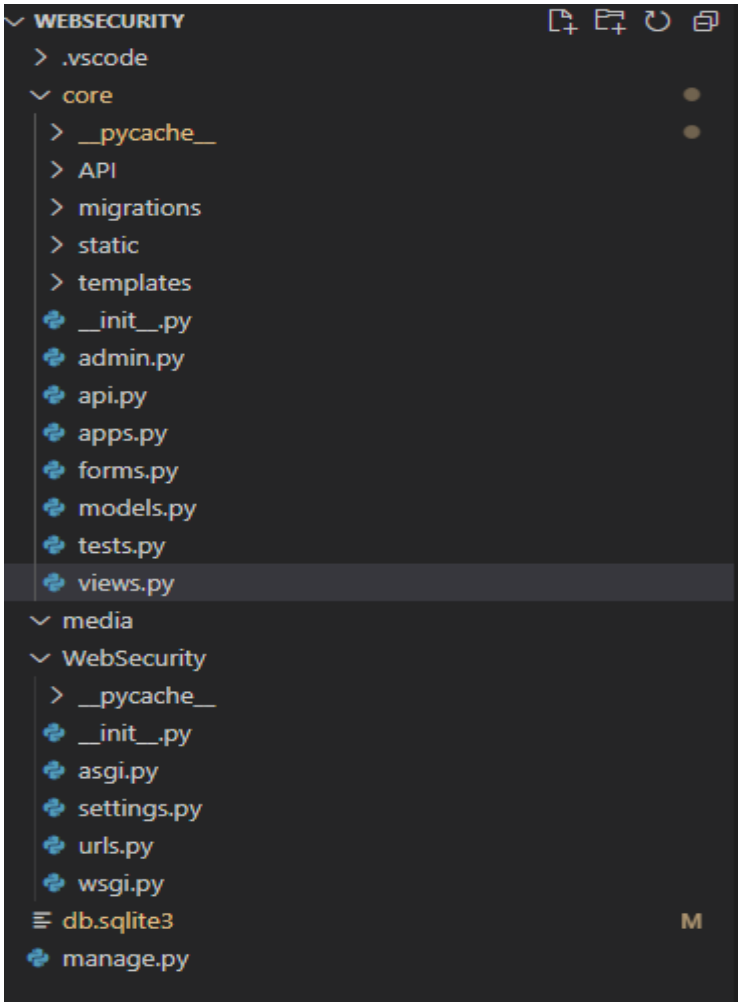


Figura 7.3.2: Imatge de l'estructura del projecte Django MVT

## 7.4 Disseny de les dades

Django suporta diverses plataformes de dades relacionals i no relacionals, en aquest cas tot i tenir una plataforma amb uns requeriments simples de dades s'ha optat per una base de dades relacional SQLite.

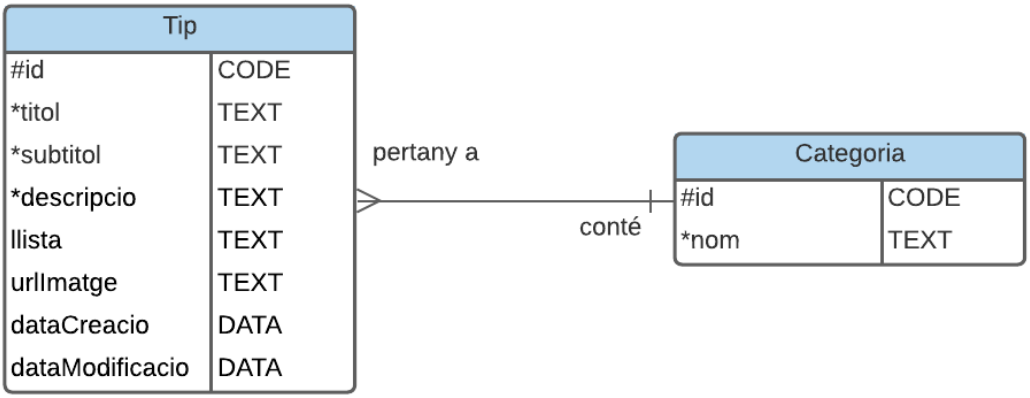


Figura 7.4.1: Model de dades de la plataforma de bones practiques.

## 7.5 Disseny de la interfície

La interfície s'ha implementat tot en una plataforma web en una sola plana dinàmica amb tres parts diferenciades:

- Plana de cerca de perillositat d'URL
- Plana de Bones pràctiques i consells contra el phishing
- Plana de mostra d'informació, comunicació i exemples reals.

**Plana de cerca de perillositat URL**

Aquesta plana és la que conté un formulari d'entrada d'una URL web i retorna un resultat del nivell de perillositat al usuari.

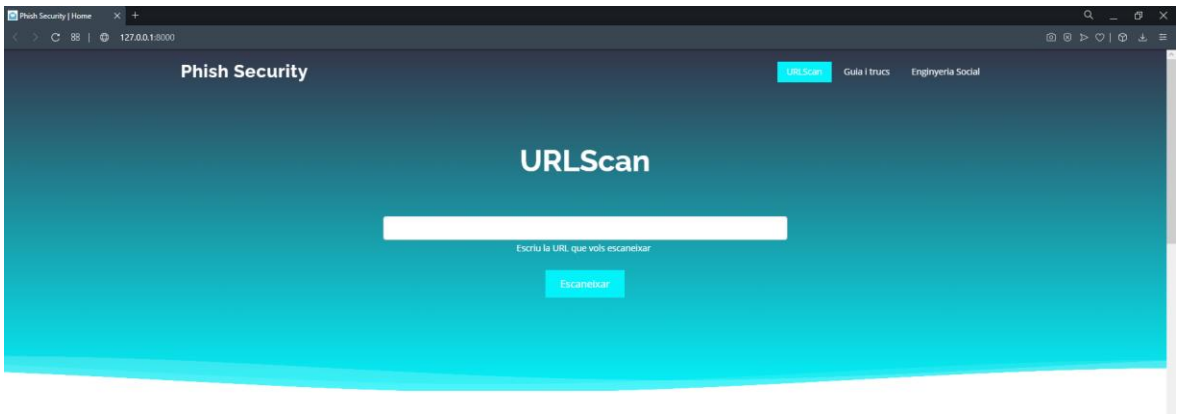


Figura 7.5.1: Plana principal de cerca de perillositat d'una URL.

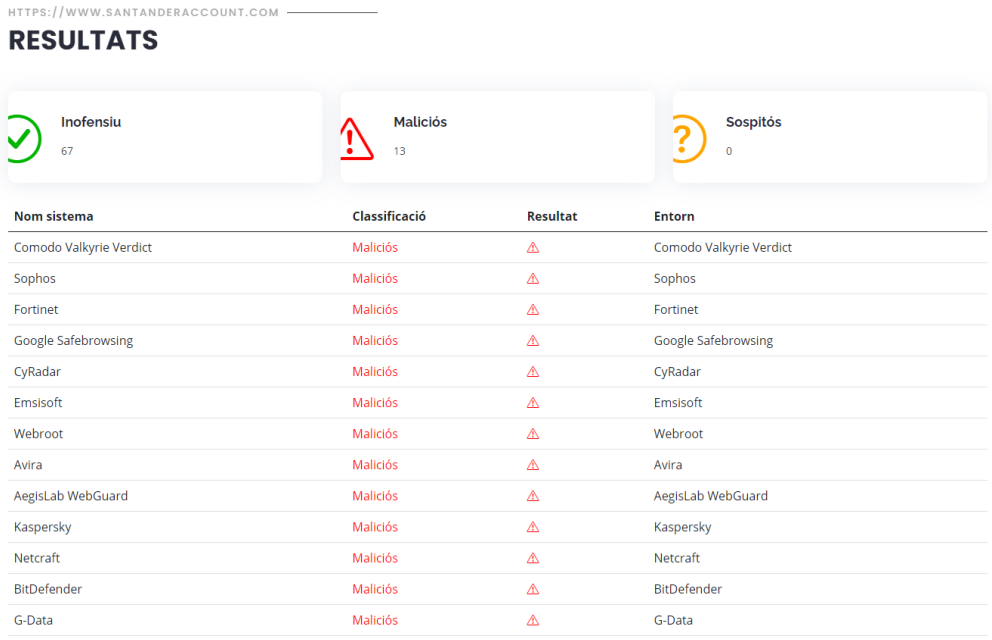


Figura 7.5.2: Plana del resultat d'una cerca url amb resultat perillós.

## Plana de bones pràctiques i consells:

Aquesta plana s'encarrega de la mostra de guies i consells a l'usuari contra el phishing electrònic.


Figura 7.5.3: Plana de guies i consells per a la protecció de l'usuari.

**Plana de mostra d'informació, comunicació i exemples reals:**

Aquesta plana s'encarrega de mostrar informació rellevant per evitar el phishing electrònic.

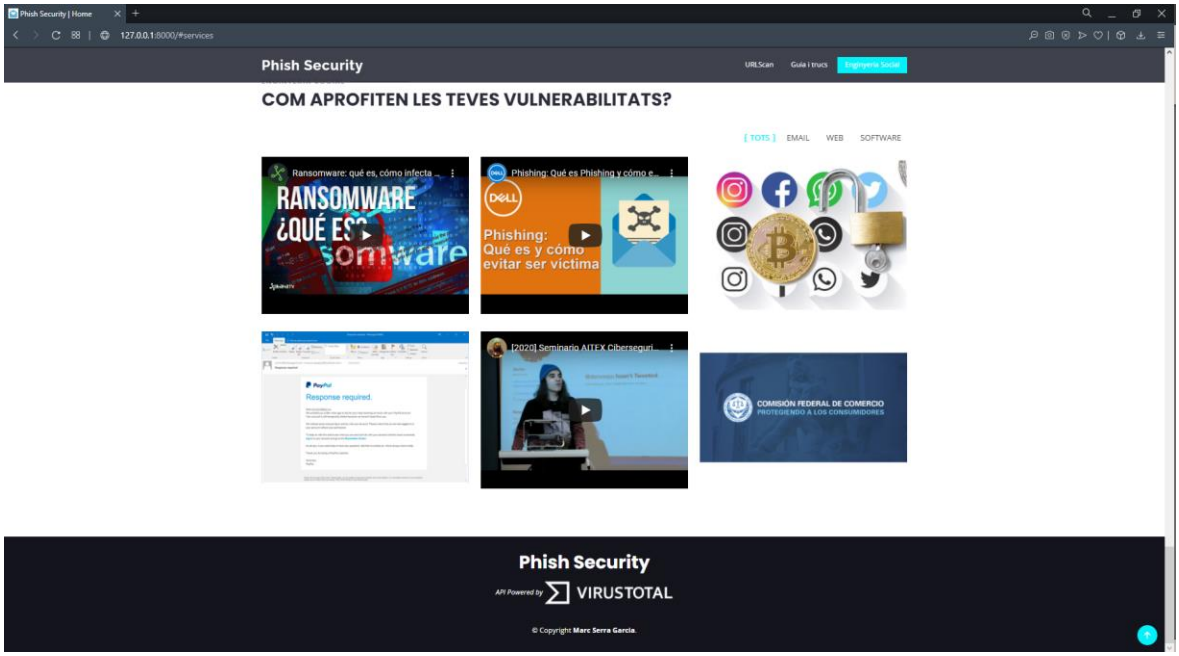


Figura 7.5.4: Plana de mostra d'informació i comunicació

# 8. Anàlisi de resultats

Com s'ha observat en l'estudi de les tecnologies phishing la facilitat d'obtenir, implementar i executar un atac de phishing en poc temps gràcies a l'existència d'eines preexistents com *Phish Kits* o la compra de software maliciós *Ransomware*. La necessitat de tenir eines de seguretat és imperativa pel funcionament dels sistemes d'informació.

Gràcies a l'estudi de les diferents característiques del phishing informàtic, s'ha complert l'objectiu de crear una llista de bones pràctiques per a la mitigació i detecció del phishing.

En quant al disseny i implementació d'una plataforma web contra el phishing, s'ha complert amb els objectius de crear una eina de detecció de enllaços web falsos. La plataforma és útil, estable, fàcilment ampliable i mantenible.

Finalment destacar l'ús de la plataforma com a eina divulgativa pels usuaris i organitzacions contra el perill del phishing electrònic.

# 9. Conclusions

En relació a l'estudi del sector i l'anàlisi de referents s'ha pogut observar que no existeix una fórmula o metodologia consistent i completament fiable contra el phishing. Tots els sistemes tenen les seves virtuts i els seus defectes, tant de detecció, com de prevenció, com de mitigació.

La volatilitat del sector del phishing, els recursos necessaris i la quantitat de sistemes informàtics fa que finalment la millor eina contra phishing i el frau electrònic és el coneixement. Ensenyar a les organitzacions i sobretot a l'usuari corrent, les eines preexistents, les causes, els mètodes de prevenció i els danys que produeixen.

En quant a la tasca de desenvolupament es pot extreure que alhora de desenvolupar una pàgina web s'ha de ser consistent en l'arquitectura, el disseny i la plataforma. Ja que una aplicació web és sovint susceptible al canvi. Tant el software, com el desenvolupador ha de ser capaç d'adaptar-se al canvi.

Finalment com amant de la informàtica crec que la ciberseguretat és un factor fonamental de la societat actual com en el futur. El projecte m'ha permès endinsar-me en el sector i posar el meu granet de sorra contra els perills que comporta el desconeixement de les tecnologies. També remarcar alguns moments de dificultat durant la gestió del projecte alhora de desenvolupar certs requeriments i finalment aconseguir resoldre totes les problemàtiques amb paciència i planificació.

# 10. Possibles ampliacions

La plataforma web pot oferir moltes possibles ampliacions de cara a un futur entre les quals hi han:

**Opció de cerca d'un arxiu o software maliciós**

Actualment la pàgina web només té l'opció de cerca d'una URL. Aquesta nova característica afegeix una nova possibilitat de l'usuari d'afegir i analitzar arxius i retornar un resultat de perillositat.

**Implementar opció de falsos positius i negatius**

La pàgina web només retorna el resultat a l'usuari i mostra en alguns casos falsos positius del anàlisi en diverses plataformes. Aquesta nova característica permet a l'usuari indicar al sistema d'un possible error de detecció.

**Ampliació d'aportacions i comentaris d'usuaris**

La pàgina web podria evolucionar a una plataforma de compartició d'eines contra el frau electrònic i el phishing. El sistema permetria a l'usuari entrar en un sistema de tipus fòrum amb una llista de temes, categories i comentaris d'altres usuaris i/o organitzacions.

# 11. Bibliografia

Anderson, R. (2008). *Security Engineering*. Wiley.

Cyberexperts. (sense data). *Cyberexperts*. Recollit de https://cyberexperts.com/history-of-cybersecurity/

ECS - European Cyber Security Organisation. (sense data). *ecs-org.eu*. Recollit de https://ecs-org.eu

Fraud Magacine. (Juny / 2013). *fraud-magazine*. Recollit de https://www.fraud-magazine.com/article.aspx?id=4294977914

INCIBE - Kit de Concienciación. (sense data). *INCIBE Protege tu empresa*. Recollit de https://www.incibe.es/protege-tu-empresa/kit-concienciacion

INCIBE - OSINT. (28 / Maig / 2014). *INCIBIE Osint-la-informacion-es-poder*. Recollit de https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

INCIBE IOCs. (sense data). *INCIBE Indicadores de compromiso*. Recollit de https://www.incibe-cert.es/blog/indicadores-de-compromiso

IOC Bucket. (sense data). *IOC Bucket*. Recollit de https://iocbucket.com

Microsoft Anti-spoof. (22 / Gener / 2021). *Microsoft anti-spoofing-protection*. Recollit de https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide

Ministeri per la Transició Ecológica. (2020). *Guía de cálculo de la huella de carbono.*

OpenIOC. (sense data). *Fire EYE*. Recollit de https://www.fireeye.com/services/freeware.html

OpenPhish. (sense data). *OpenPhish*. Recollit de https://openphish.com/

Phishtank. (sense data). *PhishTank*. Recollit de https://www.phishtank.com/

Stamp, P. P.-P. (sense data). *Handbook of Information and Communication Security*. Springer.

Talos Intelligence Cyber Attack Map. (2021). *Talos Intelligence*. Recollit de https://talosintelligence.com

Usuari kratos64. (28 / Septembre / 2018). *Github Kratos64 Phisx*. Recollit de https://github.com/kratos64/Phisx

We live Security. (16 / Febrer / 2018). *We Live security*. Recollit de https://www.welivesecurity.com/la-es/2018/02/16/phishing-mastercard-anuncios-google/