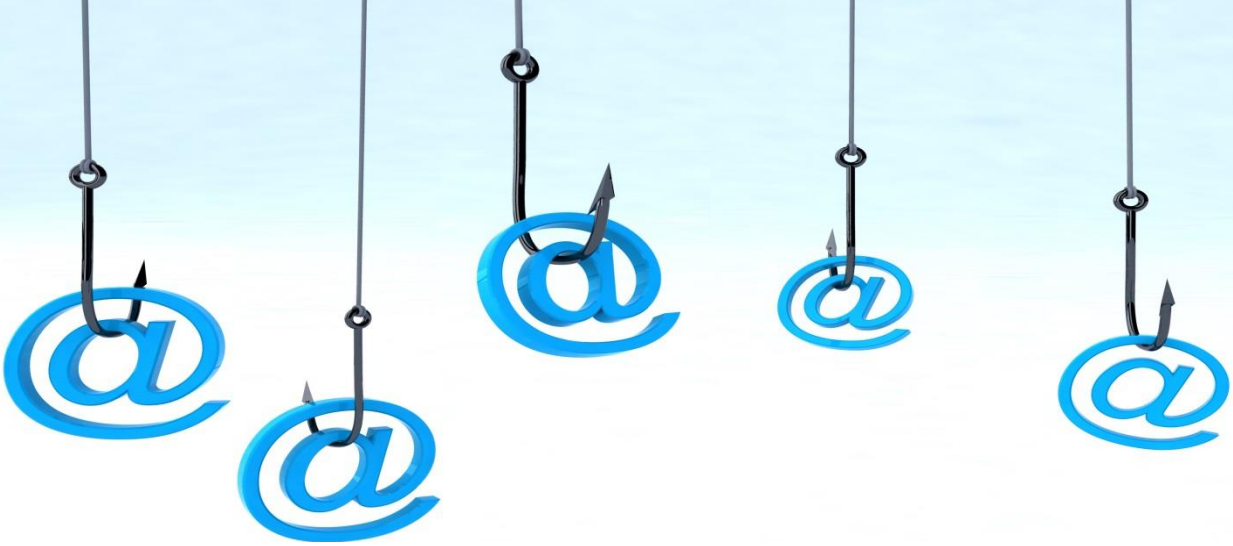
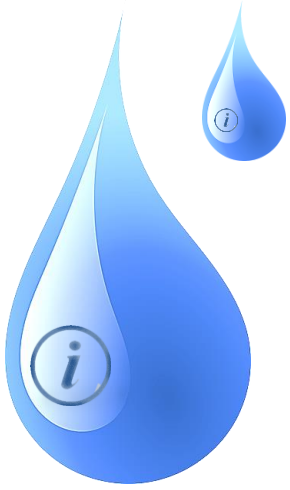


LLADRES DE DADES A L'ERA DIGITAL



TREBALL DE RECERCA

CURS: *2016 / 2017*

AUTOR: *ENRIC SIMÓ QUERALT*

GRUP: *2n BATXILLERAT*

TUTOR: *RICARD REVERTER FORCADELL*

"És natural anhelar un sentiment de total seguretat, conduint a molta gent a assentar-se en un fals sentit d'estar realment protegit. Pensa en el responsable i amo d'una casa que té un pany amb pestell instal·lada a la porta principal per protegir la seva esposa, els seus fills i la seva llar. Ell se sent satisfet en haver fet que la seva família estigui molt més segura contra els intrusos. Però, què hi ha de l'intrús que trenca una finestra o pirateja el codi de la porta del garatge? I si s'instal·lés un robust sistema de seguretat? Millor, però no és una garantia total. Amb bloquejos cars o sense ells, la casa segueix sent vulnerable.

Per què? Perquè el factor humà és en realitat la baula més dèbil de la seguretat. Al cap i a la fi, la seguretat no és un producte, és un procés".

Kevin Mitnick, *The Art of Deception (2002)*

Índex

1. INTRODUCCIÓ

1.1. Sumari

En aquest treball de recerca s'ha estudiat en profunditat un nou tòpic informàtic molt recent que està envaint la privacitat i la informació personal dels actuals internautes (ja siguin persones individualment o empreses en general). Es tracta del Phishing; un nou sistema d'atacs principalment via Internet que permeten accedir a les dades personals de tots i cadascun de nosaltres, ja siguin documents d'identitat, comptes bancaris, contrasenyes... Així doncs, **com es poden evitar aquests atacs?**

1.2. Motivació-inquietuds

Senzillament, no hi ha un únic motiu que m'hagi dut a escollir aquesta temàtica de la qual tracta el treball, són un cúmul d'interessos, curiositats i ganes de saber-ne més els qui m'han impulsat a fer-ne la recerca d'aquest món tan emocionant i a la vegada d'intriga que ens afecta constantment, molts cops sense adonar-nos de la seva gran envergadura i repercussió que pot arribar a tenir. Perquè ens afecta tan de prop? La resposta és força simple: avui dia els avenços tecnològics i informàtics arriben a tal punt d'extensió mundial que qui pugui dominar la seva extrema complexitat en la seva totalitat pot arribar a dominar el món.

Tal i com va afirmar la primera Fiscal General d'Estats Units (entre 1993-2001) Janet Reno[1] : "Tienen ordenadores, y pueden tener otras armas de destrucción masiva", els ordenadors (l'eina fonamental de la informàtica) es poden convertir en màquines que atemptin contra la persona i els seus drets si se'n fa un ús incorrecte e immoral de les seves capacitats.

Dins aquest extens món de la informàtica però, la meva idea és centrar-me en una de les branques que més pes té i pel contrari, de les que més mesures de seguretat manca. Estic parlant de l'àmbit de pirateria informàtica que atempta contra la identitat dels usuaris; **El Phishing**.

[1] Janet *Reno:* (Miami, Florida, 21 de juliol de 1938 - Miami, 7 de novembre de 2016) fou una jurista estatunidenca que va ser Fiscal General dels Estats Units en el període 1993-2001. Fou la primera dona a ocupar el càrrec de Fiscal General i la segona que ha estat més temps en el càrrec després de William Wirt

1.3. Objectius

Els objectius marcats per a aquest projecte de recerca són els següents:

- Estudiar quina és la diferència entre el hackeig i el phishing.
- Descobrir com funciona aquest tipus d'atac, perquè es fa, quin n'és el benefici...
- Analitzar la psicologia del phisher i veure com escull les seves víctimes.
- Estudiar quins són els mètodes de defensa actuals contra aquest tipus d'atacs.
- Elaborar un seguit de normes o consells per evitar els atacs a partir de la informació obtinguda i analitzada.
- Analitzar si hi ha suficient consciència sobre el phishing o altres atacs informàtics (enquestes)
- Dur a terme xerrades preventives del phishing
- Simular un atac de phishing

Preguntes i/o Hipòtesis:

- En què consisteix la pràctica del Phishing?
- Quina diferència hi ha amb el Hackeig?
- Com es poden evitar aquest tipus d'atacs?
- Fins a quin punt som conscients de l'existència d'aquesta amenaça?
- És possible l'eradicació del Phishing? Parteixo d'una visió optimista amb la qual crec possible la seva desaparició.

1.4. Àrea d'estudi i context: matèria, temps i espai

Matèria: Informàtica i enginyeria social

Temps: Aquest treball l'he començat a l'estiu de 2016, he anat treballant durant el curs quan tenia estones lliures almenys un cop per setmana i l'he acabat pràcticament a les vacances de Nadal.

Espai: Senzillament he treballat des de casa, exceptuant les xerrades que les he dut a terme a l'Institut Manuel Sales i Ferré.

1.5. Materials i recursos

Per a dur a terme el treball de recerca he necessitat l'ajuda de fonts diverses, com Internet i alguns llibres. L'eina fonamental del treball que he necessitat ha estat l'ordinador, ja sigui per elaborar la part teòrica i l'anàlisi de la part pràctica com per simular l'atac de Phishing o fer el Power Point de presentació per a les xerrades.

1.6. Metodologia

Per a poder assolir el màxim d'objectius possibles, primerament és necessari fer una recerca exhaustiva de tota aquella informació necessària per entendre en què consisteix el món del phishing. Seguidament, havent analitzat tota la informació obtinguda s'haurà de fer un procés invers, si ja es coneix en que consisteix, com es fa, per què... s'analitzarà com prevenir-ho, evitar-ho, és a dir, saber com defensar-se. Paral·lelament a l'obtenció d'aquestes dades, s'analitzarà la consciència de la gent de diferents franges d'edat sobre el tema, per veure fins quin punt estan assabentades de la possible gravetat d'un atac de phishing. Posteriorment, es posaran en pràctica els coneixements adquirits mitjançant unes xerrades a l'alumnat de 1r d'ESO per ensenyar-los els fonaments bàsics d'aquests atacs i quines són les millors maneres d'evitar-los i simulant un atac de Phishing per veure com funciona realment aquesta pràctica. Un cop acabat el projecte, s'extrauran unes conclusions que serviran de valoració i síntesi d'allò que realment s'ha assolit i allò que no s'ha pogut dur a terme.

Amb tot, s'inclouran definicions a peu de pàgina d'alguns termes difícils o desconeguts habitualment, així com imatges o petits esquemes gràfics per entendre millor els conceptes descrits.

PART TEÒRICA

2. CONTRAST. HACKING I PHISHING

En aquest apartat són tractats els dos tipus d'atacs cibernètics més famosos existents actualment; el hacking o hackeig i el Phishing o suplantació d'identitat. Primerament són explicats per separat, indicant en què consisteixen, l'origen... i finalment s'especifica la diferència clau entre tots dos. A partir d'aquesta diferència es desenvolupen els altres apartats del treball, així doncs, és molt important tenir-la present per no confondre el Phishing amb el Hacking.

2.1. Hacking

Dins aquest subapartat s'explica d'on prové (els seus orígens, tant de la paraula com del mètode en sí), la definició del terme, els prejudicis que té la majoria de gent en sentir aquest concepte i finalment quins tipus de hackers existeixen.

2.1.1. Orígens

- Origen de la paraula

La paraula "hack" significa tallar, cop de destral, així doncs s'anomenaria "hackeig" al mètode d'arreglar o detectar problemes en la computació de manera brusca o poc convencional. No té una relació directa, simplement es van associar tots dos termes per denominar aquesta metodologia informàtica.

- Origen del mètode

La persona considerada el primer "hacker" de la història va ser una dona, Grace Murray Hopper, que va crear i relacionar la paraula "bug" amb vulnerabilitat, un gran avenç informàtic fins al dia d'avui. Quan es parla dels primers hackers però, tots coincideixen de que els precursors d'aquest mètode van ser els treballadors del MIT (Institut Tecnològic de Massachucetts) ja que es dedicaven a solucionar problemes

tècnics (20 anys més tard que el descobriment de Grace Murray) seguint una sèrie de passos considerats com una metodologia "pre-hacking".

2.1.2. Definició

Quan es parla sobre "Hacking" o s'esmenta la paraula "Hacker" normalment se sol pensar en algú que té profunds coneixements sobre màquines que realitzen funcions de còmput i que, a més, són persones que realitzen coses "impossibles" per a l'enteniment de la majoria de la població, habitualment també es relacionen amb persones que es dediquen a realitzar estafes a gran escala sobre bancs i / o grans multinacionals, això per a la societat moderna, és un hacker. Tot i que les línies anteriors resultin molestes i molt desagradables, la realitat és que la cultura del Hacking es troba distorsionada per la societat i s'ha anat perdent a poc a poc l'essència del que significa realment la paraula "Hacker".

Cita de Chema Alonso, un reconegut Hacker a nivell nacional

Font: www.exito-personal.com/life-hacking/

Un hacker en l'àmbit de la informàtica, és una persona apassionada, curiosa, dedicada, lliure, compromesa amb l'aprenentatge i amb enormes desitjos de millorar les seves habilitats i coneixements tècnics. Així doncs, el Hackeig és bàsicament un seguit de gestes que utilitza un internauta amb elevats coneixements de programació per modificar, crear, implementar, millorar... de software[2]... de la manera que es vulgui.

[2] *Software*: També conegut com programari, és el conjunt dels programes informàtics, procediments i documentació que fan alguna tasca en un ordinador. Comprèn el conjunt sistemàtic dels programes d'explotació i dels programes informàtics que serveixen per a

Els límits d'aquestes gestes tenen de fronteres les polítiques de privacitat i seguretat d'allò que es vol modificar, és a dir, no és delicte en cap moment hackejar si no saltes la barrera de cap norma exposada en aquestes polítiques dictaminades en cada cas. S'ha de tenir en compte, però, que aquestes limitacions no són immutables, per tant, s'aniran modificant al llarg del temps.

2.1.3. Prejudicis socials

Molt cops, la terminologia "Hacker" presenta incertesa i desconeixement a una gran majoria de la població que no està familiaritzada amb aquest àmbit informàtic. Què fem molts cops, erròniament, quan dubtem o no coneixem alguna pràctica i ens resulta estranya? Efectivament, **malpensar** i **desconfiar**. El prejudici social típic "els hackers són delinqüents informàtics" és una afirmació totalment equívoca fruit de la manca d'informació sobre el tema i molt influenciada per la televisió o altres mitjans de comunicació que tergiversen el concepte real. L'origen d'aquesta desconfiança prové de la pràctica delictiva que es duu a terme a partir de la metodologia hacker, però no la posa en pràctica pròpiament un hacker, sinó un pirata informàtic o Cracker.

Els Crackers són aquelles persones que aconsegueixen guanyar accés a sistemes per mitjà de mecanismes agressius, com ara atacs de força bruta (cibernèticament) per a l'obtenció d'un compte d'usuari o fins i tot tècniques molt més sofisticades, com ara anàlisis i ruptura d'algorismes de xifrat, això entre altres coses. Aquest col·lectiu no es troba en la mateixa categoria que un Hacker, encara que moltes persones facin servir tots dos termes de forma indistinta, un Hacker i un Cracker no són el mateix, tot i que en moltes ocasions, comparteixen la mateixa passió i curiositat però objectius oposats.

El Phishing és una pràctica que duria a terme un tipus específic de Crackers anomenats Phishers.

2.1.4. Tipus de hackers

Existeixen tres tipus de hackers diferents, sense tenir en compte els Crackers esmentats anteriorment:

---

aplicacions determinades. El terme inclou aplicacions com els processadors de text, programari de sistema com el sistema operatiu, que fa d'interfície entre el maquinari i les aplicacions, i finalment el programari intermediari, que controla i coordina sistemes distribuïts.

Representació gràfica dels tres tipus de hackers

Font: www.google.es

- **Black Hats:**

Un Black Hat, és una classe de hacker dedicada a l'obtenció i explotació de vulnerabilitats en sistemes d'informació, bases de dades, xarxes informàtiques, sistemes operatius, determinats productes de programari, etc. Per tant són també coneguts com a atacants de sistemes i experts en trencar la seguretat de sistemes per a diversos fins (comunicant a l'empresa atacada els seus punts febles o investigant els diferents mètodes per explotar aquestes vulnerabilitats).

- **White Hats:**

Un White Hat és una classe de hacker dedicat a la correcció de vulnerabilitats de programari, definició de metodologies, mesures de seguretat i defensa de sistemes per mitjà de diferents eines, són aquelles persones que es dediquen a la seguretat en aplicacions, sistemes operatius i protecció de dades sensibles, garantint d'aquesta manera la confidencialitat de la informació dels usuaris.

- **Gray Hats:**

Un Gray Hat és una classe de hacker que es dedica tant a l'obtenció i explotació de vulnerabilitats com a la defensa i protecció de sistemes, per tant pot dir-se que un Gray Hat, freqüentment és catalogat com un hacker amb habilitats excepcionals i que les seves activitats es troben en algun punt entre les exercides pels White Hat hackers i els Black Hat hackers.

Ara bé, aquests tipus de hackers es mouen en contextos molt diversos, n'hi ha que treballen amb empreses millorant la seva protecció, d'altres col·laboren amb la policia... i una gran majoria investiga pel seu compte amb fins no perjudicials i comparteixen els seus descobriments o avenços a la xarxa amb d'altres internautes.

2.2. Phishing

Dins aquest apartat s'inclou la seva història (orígens), una completa definició del concepte i els tipus de Phishing existents actualment.

2.2.1. Orígens

- Origen de la paraula

El terme Phishing prové de la paraula anglesa "fishing" (pesca), fent al·lusió a l'intent de fer que els usuaris "mosseguin l'ham". També es diu que el terme Phishing és la contracció de password harvesting fishing (collita i pesca de contrasenyes), encara que això probablement és un acrònim retroactiu, atès que l'escriptura "ph" és comunament utilitzada per hackers per substituir la f, com arrel de l'antiga forma de Hacking telefònic coneguda com Phreaking.

- Origen de la pràctica

El primer esment del terme Phishing data al gener de 1996. Es va donar en el grup de notícies de *hackers alt.2600*, tot i que és possible que el terme ja hagués aparegut anteriorment en l'edició impresa del butlletí de notícies *hacker 2600 Magazine*. El terme Phishing va ser adoptat pels que intentaven "pescar" comptes fent-se passar per membres i treballadors d'AOL[3].

Logotip de l'empresa AOL

Font: www.google.es

2.2.2. Definició

El concepte de "Phishing" o "fer un Phishing" és potser desconegut per una gran majoria dels usuaris d'Internet, ja que normalment s'associa tot allò destinat a crear problemes informàtics o robar informació per mitjà de la xarxa als pirates informàtics o virus. En definitiva, majoritàriament es desconeix aquesta pràctica i això pot suposar la pèrdua immediata de moltes de les dades personals de qualsevol internauta.

La paraula Phishing és utilitzada per referir-se a un dels mètodes més utilitzats per delinqüents cibernètics per estafar i obtenir informació confidencial de forma fraudulenta com pot ser una contrasenya o informació detallada sobre targetes de crèdit o altra informació bancària de la víctima.

[3] *AOL*: America Online, és una empresa d'Internet i mitjans de comunicació amb la seu a Nova York que va ser la primera empresa utilitzada per al falsejament de missatges, en els quals els phishers es feien passar per treballadors d'AOL i n'obtenien comptes bancaris.

Advertència d'OIT Help; pàgina especialitzada en seguretat a la xarxa

Font: www.google.es

L'estafador, conegut com a Phisher, es val de tècniques d'enginyeria social, fent-se passar per una persona o empresa de confiança en una aparent comunicació oficial, generalment un correu electrònic, o algun sistema de missatgeria instantània, xarxes socials SMS / MMS, o fins i tot utilitzant també enquestes telefòniques. Molts cops els missatges rebuts per les víctimes, tot i aparentar total seguretat desencadenen la descàrrega d'un malware[4] que infecta l'ordinador i pot dur a terme diferents tasques:

- Copiar totes les carpetes i arxius de l'ordinador.
- Eliminar tota la informació guardada en el disc dur.
- Enregistrar totes les adreces electròniques a les quals entra l'usuari de l'ordinador afectat per veure quines pàgines freqüenta, si fa transaccions per Internet...
- Paralitzar diferents accions (ratolí, teclat...).
- Adware (virus de publicitat, Spamer)

[4] *Malware*: Fa referència a qualsevol tipus de programari maliciós que tracta d'infectar un ordinador, un telèfon mòbil o una tablet. Els crackers utilitzen el malware amb diversos propòsits, com ara extreure informació personal, el robatori de capital o impedir que els propietaris accedeixin als seus dispositius.

A més a més, venen acompanyats de posteriors missatges que demanen una suma "x" de diners si es desitja recuperar la informació, l'eliminació del virus, la recuperació d'un compte... Cal afegir que pagar ha de ser l'últim recurs, ja que ningú ens garanteixi el compliment de la promesa; al cap i a la fi el Phisher està cometent un delicte.

Exemple de Phishing:

Missatge fals (scam) d'un banc enviat per un Phisher via correu electrònic

Font: https://goo.gl/fE0cBo

2.2.3. Tipus de Phishing

Existeixen diverses maneres de fer un Phishing, totes i cadascuna d'elles destinades a l'obtenció d'informació personal de la víctima i la seva posterior suplantació d'identitat. La utilització d'un mètode o un altre és condicionada per dos factors:

- Tipus d'informació que es vol obtenir

    - *Dades personals*
        - Direccions de correus
        - Documentació d'identitat
        - Dades de localització i contacte

    - *Informació financera*
        - Número de targetes crèdit
        - Comptes bancaris
        - Informació de Home Banking o e-commerce (transaccions amb el banc via Internet i compres online)

    - *Credencials d'accés*
        - Xarxes socials
        - Correus electrònics

- A qui va dirigit el Phishing

    - *Víctimes aleatòries* (no importa qui sigui la víctima ni si "mossega l'ham")

    - *Víctimes d'un sector determinat* (es determina quin sector d'edat, gènere, país... serà l'afectat)

    - *Víctimes concretes* (s'adreça a un nombre concret i reduït de persones les quals són escollides detingudament pel Phisher, normalment de bona condició econòmica)

El mètode Phishing utilitza diversos **mitjans de propagació** o atac, el més popular i utilitzat és **via correu electrònic** (aquest mètode és explicat en profunditat en el punt 3.2) encara que n'existeixen d'altres:

- Xarxes socials

El phisher es fa passar per un amic, conegut, o algú que aparentment desitja conèixer la víctima mitjançant un perfil fals. Convenç la víctima per a que li confessi la informació desitjada, així doncs és un mètode d'àmbit concret, és a dir, s'adreça a persones no escollides a l'atzar de les quals es vol obtenir, informació personal. Majoritàriament aquest mètode no s'utilitza amb fins econòmics.

- SMS / MMS

El phisher crea un SMS o MMS on s'adreça a les víctimes com una empresa o entitat fiable, en aquest missatge demana certes dades (normalment el reenviament d'un altre SMS o MMS per part de l'afectat/da amb un text especificat pel phisher) de forma aparentment segura. Amb aquest mitjà es pretén enganyar la víctima perquè reenviï el missatge amb el text desitjat i d'aquesta manera s'haurà subscrit inconscientment a certa pàgina de Spam (correu brossa) que li cobrarà per cada SMS o MMS posterior rebut. L'àmbit al qual s'adreça generalment aquest tipus de Phishing és aleatòria.

- Enquestes telefòniques

Mitjançant enquestes telefòniques els phishers demanen l'enquestat que respongui certes preguntes d'àmbit general curosament escollides. Són del tipus:

  - Color preferit?
  - Mascotes? Quantes? Nom de les mascotes?
  - Any de naixement?
  - Dia de l'aniversari?
  - Parella? Nom de la parella?
  - Fills? Noms dels fills?
  - Població?
  - Etc.

Què pretén obtenir el phisher amb les respostes rebudes de persones concretes o d'un sector reduït escollides expressament? Segurament la persona afectada hagi escollit com a contrasenya de les seves xarxes socials, comptes, correus... alguna d'aquestes respostes, ja que molts cops proposem com a contrasenya algun tret de la nostra vida personal. El phisher recull totes les respostes i amb algun tipus de programa concret

prova totes les combinacions (ajuntant dos termes, majúscules, minúscules...) fins que n'obté la clau per accedir-hi. S'ha de tenir en compte, però, que el phisher coneix des d'un primer moment les seves adreces de correus o xarxes socials, per a posteriorment poder descobrir-ne la contrasenya.

- Infecció de malware

Aquest últim tipus és potser el fil interrelacionant entre el Crackeig generalitzat i el Phishing, ja que a més de falsificar un missatge d'un ens de confiança hi addereix un "link" o "url" que redirigeix la víctima a una nova pàgina web de descàrrega directa del virus informàtic (anteriorment s'esmenta en que repercuteixen aquests virus) i posteriorment, aquest mateix afectat rep un missatge on se l'amenaça de que haurà de pagar si vol recuperar la informació perduda o desfer-se'n del virus. Normalment aquests pagaments es fan via Paypal o d'altres transaccions per Internet (molts cops en la xarxa profunda o "Deep Web", la qual es coneix com la cara oculta d'Internet, difícil d'accedir, utilitzada amb fins il·legals...) mentre el phisher utilitza algun tipus d'ocultació de la IP (identificador únic de l'ordinador), modificadors de VPN o geolocalitzadors i d'altres mètodes per evitar ser detectat en cas de voler-li seguir el rastre i/o desemmascarar-lo. Un exemple de missatge posterior a la infecció de malware és el següent:

Víctima de Phishing afectada pel virus "Cryptolocker", el qual xifra tots els arxius de l'ordinador.

Font: https://goo.gl/Ui5QEt

Esquema dels tipus de Phishing

Font: www.infospyware.com

2.2.4. Els 3 atacs de Phishing amb més ressò a la premsa

- **eBay i PayPal**

Al maig de 2014, "eBay" sorprenia demanant als usuaris de PayPal, la pàgina web de pagaments en línia de la seva propietat, que canviessin les seves contrasenyes d'accés.

Sembla que la companyia havia confirmat que els ciberdelinqüents havien accedit, un parell de mesos abans, als comptes d'alguns empleats mitjançant la metodologia phisher. Això els hauria donat accés a la xarxa interna de l'empresa i, des d'allà, a la base de dades amb noms d'usuaris, telèfons, adreces de correu electrònic i contrasenyes.

- **Imatges d'actrius de Hollywood a la xarxa**

Al setembre de 2014 es va produir l'atac del que més s'ha parlat a la premsa: el CelebGate.

La filtració d'imatges íntimes de la guanyadora de l'Oscar el 2013, Jennifer Lawrence, així com d'altres models i actrius a través del fòrum / b / de 4Chan, va donar molt de què parlar.

Apple, va assegurar que els comptes d'aquestes "celebrities" van ser compromeses per un atac molt específic sobre els noms d'usuari, contrasenyes i preguntes de seguretat. Una pràctica amb fonaments de Phishing.

D'aquesta manera, Apple va negar que el hackeig a aquests comptes es produïssin per una vulnerabilitat en serveis com iCloud o 'Find my iPhone'.

- **Twitter**

Milers d'usuaris de Twitter van rebre missatges directes "d'amics" convidant-los a visitar un web que redirigeix a una pàgina falsa de Twitter. Des d'ella es podia robar informació dels usuaris, comprometent les seves identitats per enviar missatges de correu brossa a altres membres de la xarxa social.

Mitjançant aquest mètode els delinqüents van obtindré, a més, 33 comptes de personatges famosos, entre ells Britney Spears i Barack Obama.

2.3. Contrast. Diferència principal entre el Hacking i el Phishing

Hacking i Phishing, tot i presentar metodologies semblants que requereixen en molts casos alts nivells de coneixement de la programació, són dos àmbits informàtics totalment diferents i que no s'han de confondre. Una de les diferències més importants i notables és que tots els phishers duen a terme pràctiques fraudulentes en les quals es fan passar per fonts fiables i enganyen a la víctima per a que dugui a terme una tasca determinada. En el hackeig, en canvi, només es parla d'activitat il·legal quan s'adreça el terme equívocament als pirates informàtics que s'aprofiten de les tècniques hacker per obtenir algun tipus de benefici.

La diferència principal entre els ciberdelictes que treballen mitjançant la metodologia hacker i els phishings és simple:

"*La voluntarietat de les víctimes*"

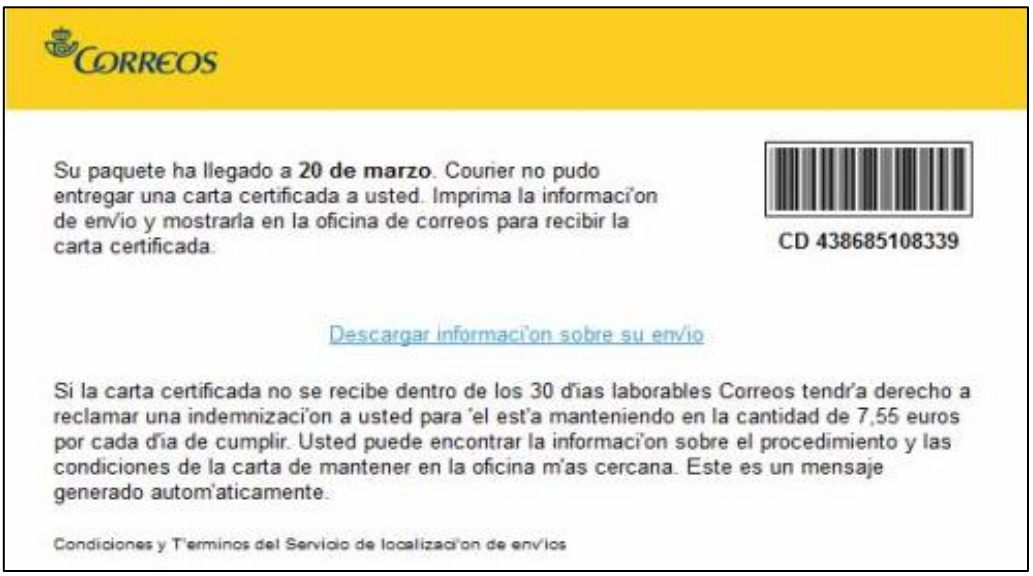
En un atac d'un pirata informàtic hacker utilitzarà diferents gestes per obtenir el seu propòsit sense que la víctima pugui fer res, mitjançant la "força bruta" sense opció per part de l'afectat a negar-se a l'atac. Els phishers, en canvi, juguen amb la innocència o suggestió de les persones atacades, mitjançant missatges o conversacions convincents, aparentment fiables, i són aquestes qui activen l'atac, qui donen la informació sense ser-ne conscients al ciberdelinqüent. Així doncs, cada cop més s'utilitza la metodologia phisher per un motiu: a l'ésser la víctima qui revela la informació "voluntàriament" és molt més difícil de rastrejar i detindre l'atacant, en canvi en el Hacking existeixen tot tipus de tallafocs o mesures anti-hack que eviten atacs i posteriorment se'ls pot seguir la pista més fàcilment, encara que són tècniques molt més efectives ja que no es depèn de si la víctima lliura la informació desitjada o no.

3. EL PHISHER

Al llarg d'aquest apartat s'explica concretament la psicologia del Phisher, és a dir, qui i com és, perquè ho fa, quin benefici en treu, quines intencions té,... A més a més, es planteja l'estructura bàsic a d'un atac phishing, el qual consta de tres parts: la selecció de les víctimes, l'elecció del mitjà de propagació segons els tipus de víctimes a les quals van destinats els atacs (on es presenta en profunditat l'exemple més popular de Phishing, via correu electrònic) i finalment un procés posterior a aquests que consisteix en l'ocultació, en evitar ser detectat o localitzat.

3.1. Àmbit psicològic

La figura del Phisher pot aparentar ser la d'una persona frívola, sense escrúpols, amb avançats coneixements d'informàtica, en ocasions de parla convincent (enquestes telefòniques o xarxes socials)... però, i si no fos només una persona? En realitat, la majoria dels atacs massius que s'han dut a terme per tot el món han estat obra d'empreses de Phishing. Es tracta d'associacions il·legals de crackers que es dediquen a l'engany i falsejament de fonts i a la seva distribució que abasteix enormes quantitats d'internautes. Normalment treballen en l'ombra, sense ser descoberts, o es coneixen pel nom del virus que trameten si aquest es fa molt famós: el virus de "Correus" per exemple.



Falsificació d'un correu electrònic de Correus amb un link adjunt de la descàrrega d'un "Cryptolocker"

Font: www.google.es

Les intencions dels phishers poden ser de dos tipus:

- **Econòmiques**

Es busca una remuneració econòmica determinada que es pot obtenir de dues maneres diferents:

  - Si es roba un compte bancari s'extreu o s'empra la quantitat desitjada d'aquell compte.
  - Si es roba un correu, perfil, s'infecta un ordinador amb algun virus... es demana a la víctima la suma de diners i com els haurà de pagar per recuperar les seves dades.

- **Personals**

En aquest cas l'interès de fer un atac de Phishing és molt concret, es busca majoritàriament la humiliació de la víctima, venjança... també es fa per entreteniment o simplement molts cops s'efectua per diversió o per demostrar les seves capacitats. Aquest últim cas es dut a terme per phishers individualment, mai una "empresa de Phishing" tindria aquestes intencions.

3.2. Metodologia phisher

Com ja s'ha esmentat en apartats anteriors, en moltes ocasions la metodologia phisher guarda molta relació amb la hacker, bàsicament es deu a que adopten tècniques d'aquesta per crear els virus, els falsos links, els missatges... les trampes que trameten en general. Per a dur a terme un atac Phishing eficient s'han de tenir en compte tres passos:

3.2.1. Selecció de víctimes

Primerament es planteja qui serà l'afectat, és a dir, a qui se li vol treure informació o quines persones tenen accés a la informació que es desitja. Tal com indica l'apartat 2.2.3. existeixen tres tipus de seleccions, el perquè s'escull una o altra és el següent:

- **Aleatòria**: Aquesta selecció és pròpia dels atacs massius elaborats per empreses dedicades a les pràctiques fraudulentes, són d'abast molt extens i la remuneració econòmica pot arribar a ser molt elevada però la eficiència o índex d'èxit és molt escàs degut a la no adequació del missatge fals per a moltes de les possibles víctimes que acaben ignorant-lo.

- **Sectorial**: Aquesta selecció és pròpia d'atacs massius especialitzats duts a terme per empreses de Crackeig, que duen a terme tot tipus de pràctiques ciberdelictives. L'eficiència d'aquests atacs és molt més elevada i per tant són més difícils d'evitar o descobrir ja que saben exactament a quina franja d'edat, sexe, comunitat, país... van dirigits.

- **Concreta**: Aquesta selecció és pròpia d'atacs estudiats detalladament, preparats i elaborats gairebé a la perfecció. Els falsos missatges gaudeixen d'un vocabulari convincent, proper al receptor, dirigit expressament a ell, el qual li resultarà familiar, segur i fiable. L'índex d'èxit amb aquesta selecció és molt elevat, i s'adrecen normalment a empreses o persones d'una condició econòmica important. Tot i això, cada cop més les empreses posen a prova tècniques per evitar aquest tipus d'enganys i estafes, encara que en moltes ocasions els atacs són impecables i són molt difícils d'evitar.

3.2.2. Mitjà de propagació

Posteriorment, quan el phisher ja sap a qui ha de dirigir el ciberatac, selecciona quin mitjà de propagació és l'adient per al tipus de víctimes que ha escollit. Els diferents mitjans són els explicats en l'apartat 2.2.3.

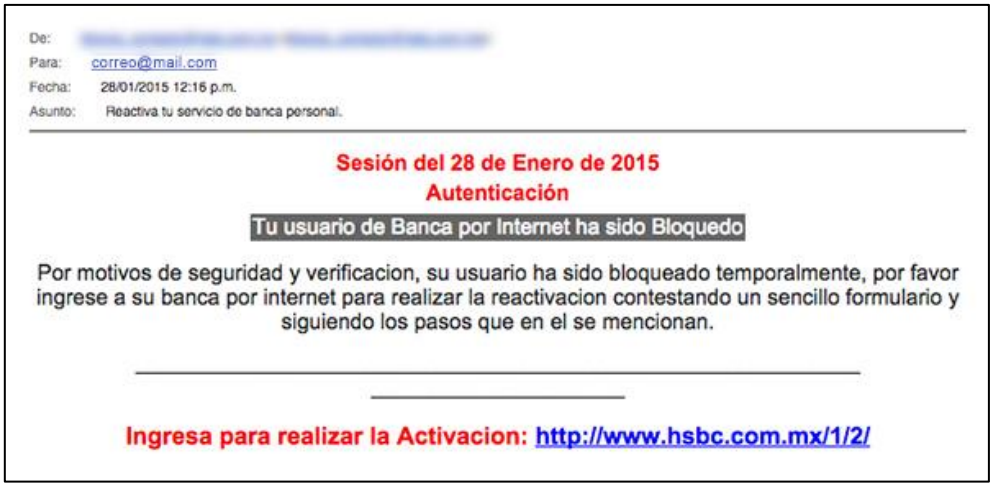
Selecció aleatòria	Selecció sectorial	Selecció concreta
Correu electrònic	Correu electrònic	Correu electrònic
SMS / MMS	Xarxes socials	Xarxes socials
Infecció de malware	Infecció de malware	Enquestes telefòniques
		Infecció de malware

Com es pot apreciar en la taula, el mitjà del correu electrònic s'utilitza en tots tres àmbits, és el més popular, efectiu i fàcil de realitzar. A més, la infecció de malware va normalment incorporada en els missatges via correu electrònic, així doncs mentre s'utilitza aquest mitjà de propagació s'infecta amb un virus informàtic l'ordinador de la víctima.

3.2.2.1. Via correu electrònic

El correu electrònic és l'eina principal de treball dels phishers, la qual ha protagonitzat atacs massius que eleven les xifres a milions d'afectats en tot el món. El circuit d'atac per aquest mitjà consta de 5 fases:

a) Falsificació d'un ens de confiança i creació d'un correu convincent, aparentment fiable i concís.



De: [redacted]
Para: correo@mail.com
Fecha: 28/01/2015 12:16 p.m.
Asunto: Reactiva tu servicio de banca personal.

Sesión del 28 de Enero de 2015
Autenticación

Tu usuario de Banca por Internet ha sido Bloquedo

Por motivos de seguridad y verificacion, su usuario ha sido bloqueado temporalmente, por favor ingrese a su banca por internet para realizar la reactivacion contestando un sencillo formulario y siguiendo los pasos que en el se mencionan.

Ingresa para realizar la Activacion: http://www.hsbc.com.mx/1/2/

Falsificació d'un ens real

Font: www.google.es

b) Distribució del correu segons la selecció de víctimes que s'ha fet.

- Els correus es poden obtenir de dues formes:

  i. Si es coneix la víctima el més segur és que el phisher tingui al seu abast el seu correu electrònic o bé el pugui trobar amb facilitat.
  ii. Si es pretén fer un atac massiu i es necessiten grans quantitats de correus els phishers recorren a fòrums, cadenes d'e-mails, pàgines de spam que faciliten correus... i sobretot a les filtracions produïdes per crackers i compartides a la xarxa profunda (Deep Web).

c) Un cop les víctimes han rebut els correus, un petit percentatge l'obre i confia amb el que diu, voluntàriament fan "click" a l'enllaç proporcionat que pot redirigir a dos opcions:

- Accés a una web falsa[5] creada pel phisher on s'introdueixen les dades demanades.
- Descàrrega d'un malware (adware, cryptolocker...)

[5] *Web falsa (scam)*: Es tracta de pàgines web creades pels phishers que aparenten ser les pàgines d'inici de sessió de xarxes socials, comptes, bancs... de confiança. Moltes vegades la diferència entre la vertadera i aquesta és pràcticament inexistent ja que s'utilitza el mateix format per crear-la.

d) El phisher obté les dades (si s'ha utilitzat la web falsa) o envia un altre correu on especifica la quantitat de diners que vol rebre i com la vol rebre mitjançant una sèrie d'instruccions (si es produeix una infecció amb un virus informàtic).

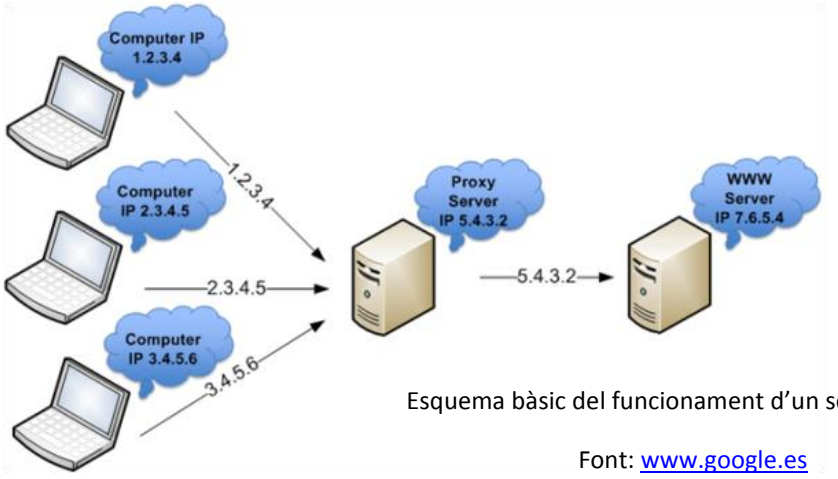
3.2.3. Ocultació. Tècniques post-Phishing

Existeixen moltes tècniques d'ocultació que utilitzen els phishers més experimentats que consisteixen en mètodes molt complexos de romandre en l'ombra, d'ésser indetectables, esborrar el rastre per a que ningú pugui investigar els seus actes i no poder ser detinguts mai. Són tècniques que s'utilitzen posteriorment a un atac o durant aquest. Tres dels mètodes més coneguts són:

- Canvis i ocultació d'IP

L'adreça IP és un nombre que identifica inequívocament un dispositiu lògic connectat a la xarxa. Dins d'una mateixa xarxa, cada adreça IP que s'utilitzi ha de ser única. Existeixen IPs dinàmiques (poden canviar) i estàtiques (no poden canviar).

En aquest cas es combinen els canvis d'aquests nombres i la seva ocultació mitjançant un servidor Proxy[6] o altres dispositius que permetin enviar informació ocultant el número d'identificació de l'ordinador de l'emissor.



Esquema bàsic del funcionament d'un servidor Proxy

Font: www.google.es

[6] *Servidor Proxy*: és un servidor -programa o dispositiu-, que fa d'intermediari en les peticions de recursos que realitza un client (A) a un altre servidor (C). Per exemple, si un hipotètic phisher A sol•licita un recurs a C, ho farà mitjançant una petició a B (el servidor Proxy), que al seu torn traslladarà la petició a C; d'aquesta manera C no sabrà que la petició va procedir originalment d'A.

- Modificadors de VPN o geolocalitzadors

Una xarxa privada virtual (VPN) és una tecnologia de xarxa que permet connectar diversos dispositius com si es trobessin físicament al mateix lloc, emulant connexions de xarxa local. Accedir a una VPN d'un altre país o continent permet saltar-se qualsevol restricció geogràfica, permetent connectar amb ordinadors d'arreu del món. A més, és un altre mètode d'ocultació de la IP i permet amagar les dades de navegació, fet que capacita el phisher per, si en un hipotètic cas en el qual se li detectés la IP, aparèixer localitzat geogràficament en l'indret d'on provingués la VPN.

Representació gràfica d'una xarxa privada virtual (VPN)

Font: www.imdigital.es/redes-y-comunicaciones/vpn/

- Els bitcoins o cryptomonedes

També anomenada "la moneda que controlen tots i ningú a la vegada", el "bitcoin" és la moneda totalment virtual que es basa en la tecnologia P2P (no importa la plataforma software ni localització que s'utilitzi per establir una connexió entre dos còmputs), va arribar fa uns anys per canviar el paradigma monetari. Es tracta d'un sistema de comerç descentralitzat i autoregulat, sense un banc central que el supervisi, s'afirma que està cridada a convertir-se en la moneda de referència mundial.

No s'imprimeix en bitllets ni s'intercanvia a través de monedes metàl·liques. Són xifres en una base de dades. Transaccions. Neix fonamentalment com a moneda per a Internet, i a diferència d'altres divises no està sotmesa a una autoritat central ni a intermediaris.

Imatge del Bitcoin, la moneda virtual descentralitzada

Font: www.coindesk.com

El seu **valor** es correspon bàsicament a dos factors: la confiança dels usuaris i el volum d'ús en la compra per Internet. Té un preu i un valor, que són dos indicadors diferents. El primer expressa el valor de la moneda virtual a partir d'una oferta i una demanda en el mercat, exactament com passa amb altres divises. El segon indicador assenyala la popularitat que la moneda virtual té entre els usuaris, i d'aquí depèn el seu èxit o fracàs. Fa menys de deu anys, el valor del bitcoin era de tot just uns cèntims d'euro. Actualment la moneda virtual val 791,47 €. Avui en dia hi ha en circulació més de 20 milions de bitcoins.

Gràfic lineal de l'evolució del valor del BitCoin en euros durant l'any 2016 fins avui dia 21 de desembre a les 15:52

Font: http://es.investing.com/currencies/btc-eur-advanced-chart

El **phisher**, posteriorment a la infecció de l'ordinador de la víctima, li demana una quantitat "x" de diners que haurà de pagar amb bitcoins, ja que al no estar regulada ni supervisada, el rastrejament de la transacció és gairebé impossible. Si l'afectat decideix pagar, haurà de comprar monedes virtuals i realitzar el pagament amb elles.

4. ANTI-PHISHING

Aquest és potser l'apartat més important del treball, l'objectiu principal del qual és, a partir de la informació obtinguda fins ara, extreure mètodes o solucions per evitar aquests atacs o detectar-los més fàcilment. L'anti-Phishing consta de dues fases, la identificació de l'atac i la resposta que s'aplica.

Cal remarcar que un atac informàtic, ja sigui un virus, una suplantació d'identitat... són amenaces d'origen molt recent, i per tant encara desconeguts per a la gran majoria d'internautes. Habitualment es comparen aquestes amenaces amb les noves malalties que han anat apareixent al llarg del temps, fins que no atempten contra un cos o varis (en aquest cas diferents ordinadors particulars, mòbils, pàgines web, empreses...) es molt difícil o gairebé impossible estudiar-les i per tant determinar-ne una solució o una prevenció d'aquesta.

4.1. Fase 1: Protecció i identificació de l'atac

La primera fase del procés Anti-Phishing és el pilar d'una bona defensa d'aquests atacs, consisteix en detectar si allò que estem rebent per missatge, trucada, correu... és fiable o no, per un senzill motiu: no donar informació personal a algun possible estafador.

Després d'haver analitzat en què consisteixen els atacs, com es fan, com operen els Phishers i per què, com escullen les seves víctimes, etc. i basant-me en les solucions proporcionades per empreses molt importants a nivell de seguretat i privacitat en la xarxa, es pot elaborar el que podríem anomenar com el **decàleg de l'Anti-Phishing.**

Aquest decàleg consta de deu breus normes o consells que calen tenir en compte a l'hora de lliurar informació personal o navegar per Internet.

- Comprovar sempre la URL[7] del lloc des d'on iniciem sessió sigui segura, la real.

Url amb http (protocol de transferència d'hipertext) que denota fiabilitat

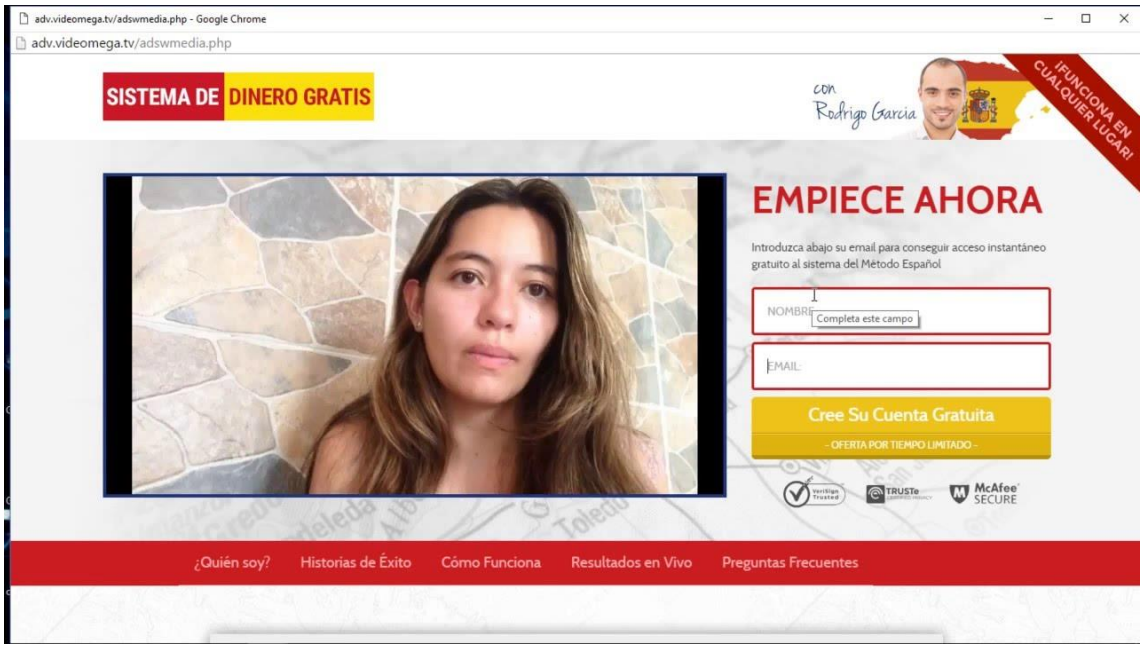
Font: www.google.es

- Sempre que ens arribi un missatge demanant-nos que iniciem sessió comprovar qui és l'emissor.

- No omplir mai enquestes d'informació general que demanin correus. És possible estar posant la pròpia contrasenya sense adonar-nos-en (al igual que en les enquestes telefòniques de qüestions generals).

- No donar dades importants a ningú que no sigui de confiança encara que ens prometi alts beneficis (per exemple els hackers de videojocs, o pàgines que prometen softwares que autònomament generen diners).

[7] *URL*: Localitzador uniforme de recursos. És una adreça formada de caràcters alfanumèrics que indica la localització d'un fitxer o d'un directori a Internet i que permet d'accedir-hi.



Pàgina de "sign up" o registre de "Shutterstock" on prometen proporcionar un software de compravenda automàtic que genera temptadores sumes de diners en poc temps. A part de ser una estafa, utilitza "brokers" o programes d'inversió il·legals i vídeos testimonials (esquerra de la imatge) d'actors pagats que afirmen la seva fiabilitat i inciten a lliurar els comptes bancaris.

Font: www.google.es

- Verifica la font que et demana dades si sospites (molt comú en els fòrums) entrant al seu perfil, analitzant els comentaris del públic, el seu historial...

- En cas d'entrar a la web del teu banc per internet MAI entris des d'un enllaç directe (proporcionat per Google o altres) sempre s'ha d'escriure al buscador l'adreça completa.

- Reforça sempre la seguretat: dispositius desconeguts, localització, petició doble de contrasenya... Generalment les xarxes socials, comptes... et donen l'opció d'aplicar aquestes tècniques en la secció de configuració i és totalment recomanable.

- Revisa periòdicament els comptes encara que no els usis i canvia, si ho veus necessari, alguna contrasenya.

- És recomanable que les contrasenyes tinguin minúscules, majúscules i números.

Existeixen una gran quantitat de programes informàtics dedicats a provar infinitat de combinacions de lletres i números amb el fi de descobrir una contrasenya. La majoria dels programes segueixen uns patrons comuns (comencen amb tot minúscules, seguidament amb tot majúscules, després amb números, més tard amb combinacions de majúscules i minúscules, majúscules minúscules i números...) si combinem els tres tipus en la contrasenya obligarem aquests programes a que hagin de trigar més temps en descobrir-la. Molts cops els Crackers que els utilitzen el programen per a que no estigui més d'un temps determinat en intentar desxifrar una clau, ja que sinó no li seria rentable. Així doncs com és complexa la tinguem, en cas d'un intent d'atac podríem sobrepassar el límit de temps i lliurar-nos-en. Afegir símbols és donar un pas més de seguretat, ja que molts d'aquests softwares no tenen les possibles combinacions amb aquests predeterminades.

Descripció gràfica del funcionament dels softwares per desxifrar contrasenyes.

Font: www.google.es

- Llegeix bé allò que et demanen, freqüentment els missatges són traduccions i és fàcil detectar la manca de claredat lingüística. Les fonts segures envien missatges sense errades ni traduccions deficients.

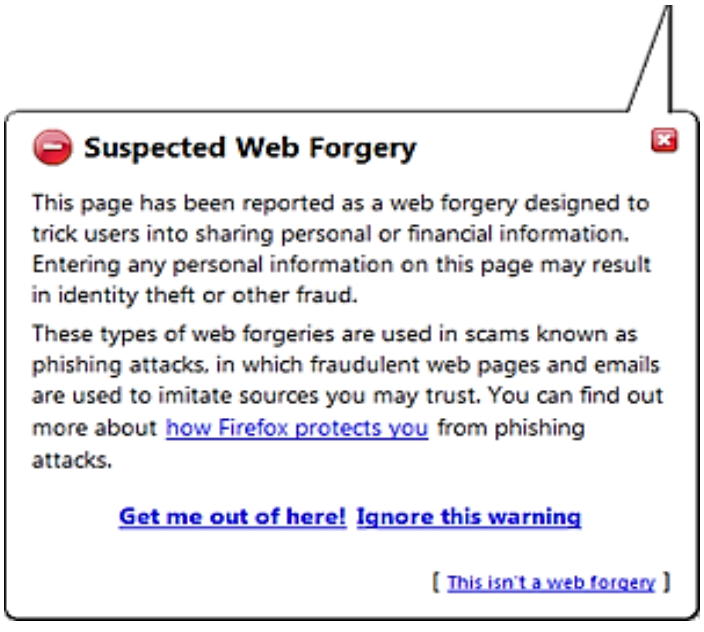
✓ La millor eina per evitar els atacs de Phishing és el **sentit comú**. Amb aquest i els consells anteriors és facilita molt detectar les possibles amenaces.

4.2. Fase 2: Respostes

Posteriorment a la identificació de l'atac, la fase següent consisteix en emetre una resposta, posar-hi una solució. Per a la majoria d'usuaris habituals el més recomanable és ignorar i eliminar qualsevol correu, missatge... sospitós. En altres casos existeixen tres tipus de d'accions per fer front al Phishing:

Resposta organitzativa: Consisteix en entrenar un conjunt de gent empleada d'una empresa o institució important per a la identificació i defensa d'atacs Phishing. Aquest grup està format per gairebé tots aquells qui participen en tasques que requereixin l'ús d'ordinadors o telefonia mòbil. D'aquesta manera l'empresa en general és conscient dels possibles atacs i es sap perfectament com detectar-los i que fer en cas de rebre'n.

Resposta tècnica: Un pas més n'és l'ús de programes especialitats en la defensa d'atacs de Phishing o Spam (publicitat), els quals realitzen funcions semblants als antivirus però dedicats exclusivament a aquests tipus d'amenaces. Serveixen com una mena de filtre de pàgines web o correus, i treballa analitzant els llocs de procedència, la fiabilitat, el contingut...



Avís de possible pàgina de Phishing d'un programa d'Anti-Phishing incorporat al navegador Firefox

Font: https://es.wikipedia.org

Resposta legislativa i judicial: Aquesta última resposta és duu a terme generalment pels cossos d'investigació cibercriminal, en els quals es desemmascara el phisher i es porta davant la justícia el delinqüent per a que sigui condemnat. És una tasca molt difícil degut a la gran quantitat de possibilitats que tenen els phishers per amagar la seva identitat, i tot i els avenços tecnològics existents segueix sent molt complex enxampar els culpables d'aquest tipus d'atacs.

5. CONSEQÜÈNCIES PENALS

El Phishing, en moltes ocasions, no es considerat un delicte en alguns països degut a que els seus atacs són tant recents que encara no s'ha considerat la possibilitat d'afegir-los com a delictes en les seves legislacions o encara estan treballant-hi. Tot i així, ara per ara ja ocupa un lloc en els delictes de frau i estafes per Internet en diversos països com Estats Units, Argentina, Espanya, Alemanya o Xile (en aquest últim no es considera directament el Phishing en cap tipus de codi penal, però es castiga mitjançant la figura de l'estafa tradicional. En general, els països que aposten per castigar aquest tipus de conductes apliquen en les seves legislatures el conveni cibercriminal de Budapest (es pot trobar a: https://goo.gl/EFy9ma)

5.1. Conveni cibercriminal de Budapest

L'ús de termes com delinqüència informàtica, cibercriminalitat, delictes informàtics, etc., s'ha convertit en una constant en la nostra societat actual. El naixement i la ràpida difusió de les xarxes informàtiques, estan propiciant que la cibercriminalitat sigui un dels àmbits delictius de més ràpid creixement.

La rapidesa, l'anonimat, la comoditat i l'amplitud d'abast que faciliten les noves tecnologies, fan que els delinqüents les aprofiten per dur a terme diverses activitats il·legals, tant tradicionals aprofitant els nous mitjans, com altres noves nascudes dins d'aquest àmbit.

Atacs contra sistemes informàtics, robatori i manipulació de dades, usurpació d'identitat, activitats pedòfiles, estafes comercials i bancàries mitjançant diferents tècniques com el Phishing, difusió de malware, creació de botnets per a diferents fins,

etc., constitueixen part d'aquestes activitats delictives comeses utilitzant mitjans informàtics.

L'abast mundial i la ràpida difusió d'aquest tipus d'activitats han causat que governs de tot el món comencin a implementar en les seves legislacions mesures per combatre-les i tractar d'evitar i prevenir els efectes nocius que puguin causar en els seus ciutadans. D'aquesta necessitat de paralitzar o minimitzar els atacs cibernètics neix el Conveni cibercriminal de Budapest.

El Conveni sobre cibercriminalitat o Conveni de Budapest és el primer tractat internacional que busca fer front als delictes informàtics i els delictes a Internet. Espanya va ratificar aquest conveni l'1 d'octubre del 2010. Les conductes il·lícites definides en aquest Conveni i traslladades a la nostra legislació són les següents:

1. **Delictes contra la confidencialitat, la integritat i la disponibilitat dels dades i sistemes informàtics.**
    a. Accés il·lícit
    b. Intercepció il·lícita
    c. Interferència de dades
    d. Interferència en els sistemes
    e. Abús dels dispositius

2. **Delictes informàtics (*Phishing i Crackeig entre d'altres*)**
    a. Falsificació informàtica
    b. Frau informàtic

3. **Delictes relacionats amb el contingut**
    a. Pornografia infantil
    b. Mercats negres
    c. Servei Hacker

4. **Delictes relacionats amb infraccions de la propietat intel·lectual i dels drets afins.**
    a. Amenaces i coaccions

PART PRÀCTICA

6. ENQUESTES

Com ha primera part pràctica d'un total de tres del treball de recerca apareixen les enquestes, uns qüestionaris per a conèixer l'opinió d'una mostra representativa de població.

6.1. Objectiu

L'objectiu fonamental d'aquestes enquestes és bàsicament veure fins a quin punt en som conscients de l'abundància i gravetat dels atacs cibernètics, i concretament analitzar si el Phishing és un terme conegut o no. A més, un altre objectiu és determinar si influeix en el coneixement d'aquests successos el gènere o edat dels enquestats. Finalment caldrà valorar si s'opina que és o no interessant i/o necessària una xerra informativa i preventiva sobre el Phishing.

6.2. Metodologia

Per a dur a terme les enquestes s'ha utilitzat el mètode tradicional, enquestes físiques. Consten d'un total de 8 preguntes que combinen resposta múltiple i oberta. Per a que l'enquestat pugui entendre el perquè d'aquesta hi ha una petita introducció al principi on també s'indiquen les instruccions a seguir. Amb tot, s'han elaborat un total de 150 enquestes, 50 per a cada franja d'edat marcada (12-16 / 17- 40 / 40 o +). El perquè d'aquestes franges és simple: la primera franja s'ha considerat com un període d'iniciació informàtica en el qual és possible que els coneixements en qüestió encara no s'hagin assolit del tot, la segona franja és considerada com l'etapa de maduresa intel·lectual en aquest àmbit, i per últim, la franja de 40 o més anys està formada per la gent que normalment no tindrà una base d'aquest tema suficientment àmplia tret que hagin estudiat o adquirit els coneixements degut als estudis o la feina que exerceixen.

6.2.1. Format

Hola! Sóc Enric Simó, alumne de 2n de Batxillerat i necessito la teva ajuda. Et formulo aquesta enquesta relacionada amb el meu treball de recerca, t'asseguro que no trigaràs més de 2-5 minuts en contestar-la. Marca amb una "X" les respostes que apareixen amb un requadre com aquest: ☐ Recorda encerclar la franja d'edat en la qual et trobes i contestar les preguntes de resposta oberta amb la major sinceritat possible (l'enquesta és anònima). Moltes gràcies!

Franja d'edat: 12 – 16 17 – 40 40 +

1. **Coneixies la pràctica del phishing ?**

☐ Sí ☐ NO

*En cas negatiu passa a la pregunta número 3

2. **Creus que els pirates informàtics (hackers) i phishers són el mateix?**

☐ A) Sí, els dos actuen amb un objectiu comú.
☐ B) No, són dues pràctiques totalment diferents.
☐ C) No, tenen una pràctica semblant però interfereixen en els seus objectius.

3. **Creus que tots els hackers duen a terme pràctiques fraudulentes?**

☐ Sí ☐ No

4. **I els phishers?**

☐ Sí
☐ No
☐ No ho sé

5. **Coneixes o has sentit mai parlar d'algun cas d'atac cibernètic contra la identitat de la persona, empresa, pàgina web... és a dir, un atac de phishing?**

☐ A) Sí, jo n'he patit.
☐ B) Sí, n'he sentit parlar.
☐ C) No, no en conec cap.

*En cas afirmatiu (respon i passa a la pregunta 7): Quin cas coneixes o has patit? _____

_____

_____

6. **Un atac de phishing pot succeir simplement en la usurpació d'un compte d'alguna xarxa social com Facebook, Instagram, Twitter, etc. Ara doncs, en coneixes algun cas?**

- ☐ A) Sí, jo n'he patit.
- ☐ B) Sí, n'he sentit parlar.
- ☐ C) No, no en conec cap.

*En cas afirmatiu: Quin cas coneixes o has patit? _____

_____

7. **Quin mètode o mètodes creus que serien efectius per evitar aquests atacs o almenys posar-hi una mica més de seguretat?**

*Exemple: Comprovar sempre que el lloc des d'on Iniciem Sessió o ens Registrem sigui segur.

_____
_____
_____

8. **Creus necessària o interessant una xerrada informativa sobre el Phishing i com evitar-lo?**

☐ Sí ☐ No

*Després de contestar tota l'enquesta, si hi estàs interessat pots llegir-te aquesta definició sobre *EL PHISHING*: Es refereix a un dels mètodes més utilitzats per delinqüents cibernètics per estafar i obtenir informació confidencial de forma fraudulenta com pot ser una contrasenya o informació detallada sobre targetes de crèdit o altra informació bancària de la víctima.

Gràcies per la col·laboració!

Què és el phishing?

6.3. Resultats i anàlisi

Franja d'edat	12 - 16	17 - 40	40 o +

Pregunta 1	Sí	No	Sí	No	Sí	No
	5	45	17	33	3	47

Pregunta 2	A	B	C	A	B	C	A	B	C
	3	0	2	10	3	4	3	0	0

Pregunta 3	Sí	No	Sí	No	Sí	No
	39	11	13	37	31	19

Pregunta 4	A	B	C	A	B	C	A	B	C
	12	6	32	28	6	16	6	0	44

Pregunta 5	A	B	C	A	B	C	A	B	C
	3	16	31	18	21	11	1	24	25

* Respostes obertes comentades a les conclusions

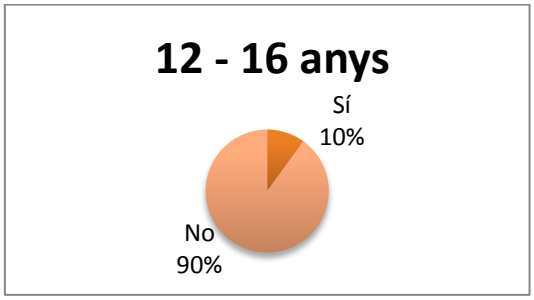
Pregunta 6	A	B	C	A	B	C	A	B	C
	8	20	4	2	9	0	0	18	7

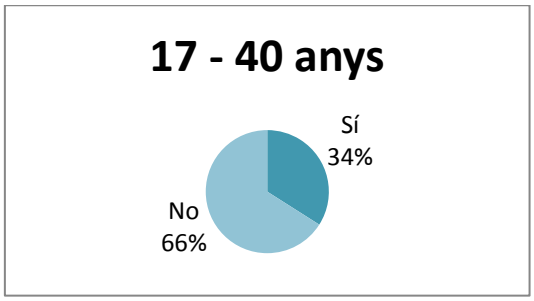
* Respostes obertes comentades a les conclusions

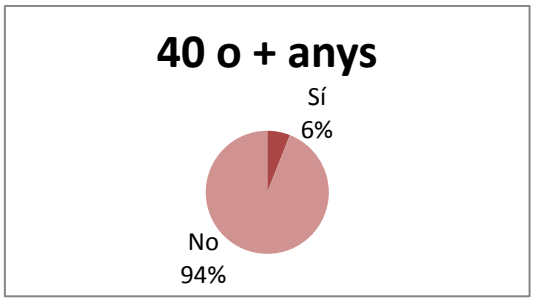
Pregunta 7	Resposta oberta

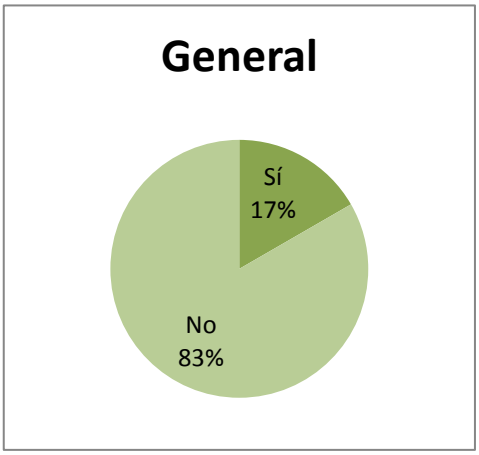
Pregunta 8	Sí	No	Sí	No	Sí	No
	49	1	50	0	44	6

Pregunta 1: Coneixies la pràctica del Phishing?





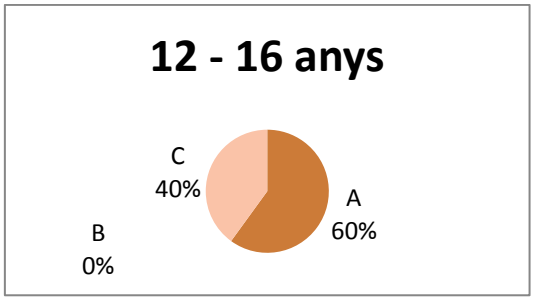


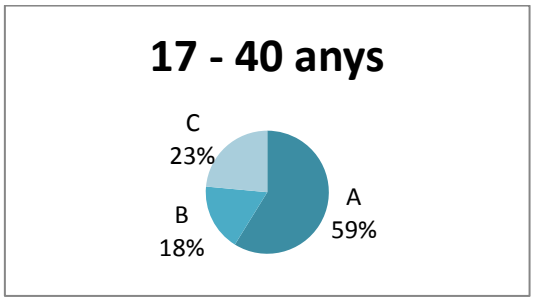


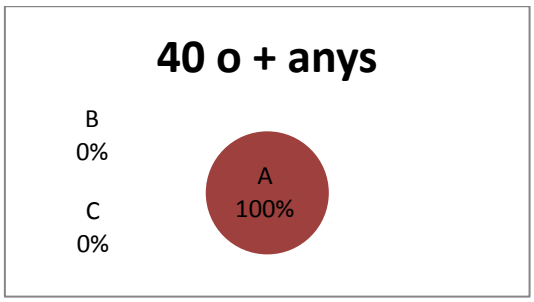
En aquesta primera pregunta s'observa fàcilment com el Phishing no és un terme conegut en la nostra societat, tot i que si analitzem detingudament les tres franges d'edat per separat la menys conscient sobre aquest tipus d'atacs n'és la de més de 40 anys, entre 12 i 16 presenten tan sols un 4% més, és a dir només un de cada 10 nois/es d'aquesta edat coneixen que és el Phishing. En canvi en l'etapa intermèdia d'edat trobem un 34%, un percentatge força elevat si es compara amb els altres dos gràfics.

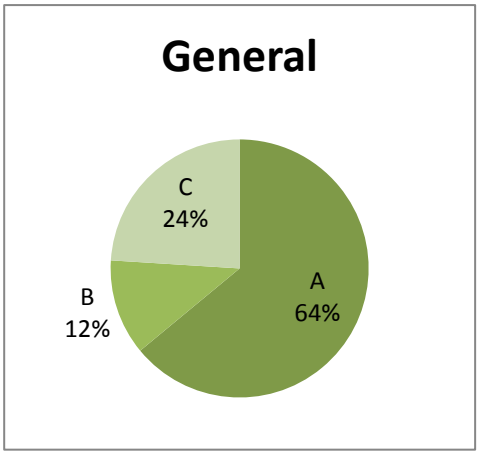
Pregunta 2: Creus que els pirates informàtics (hackers) i els phishers són el mateix?

* Aquesta pregunta només la responien aquells qui contestaven "Sí" a la pregunta 1.



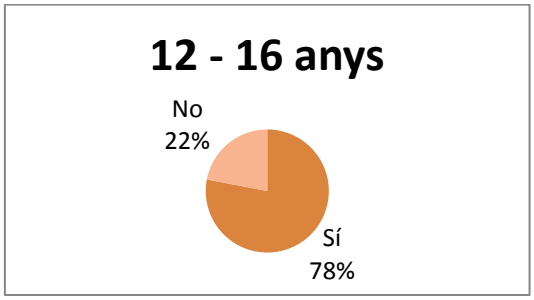


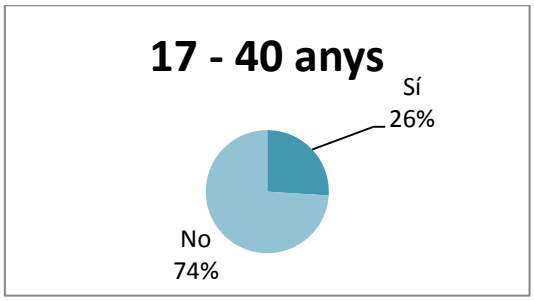


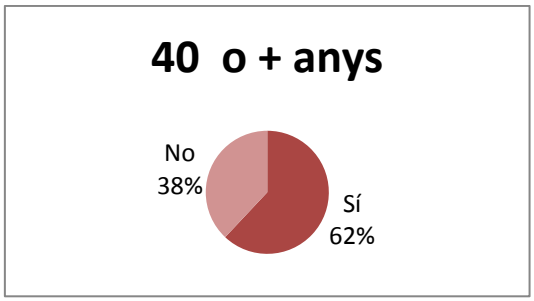


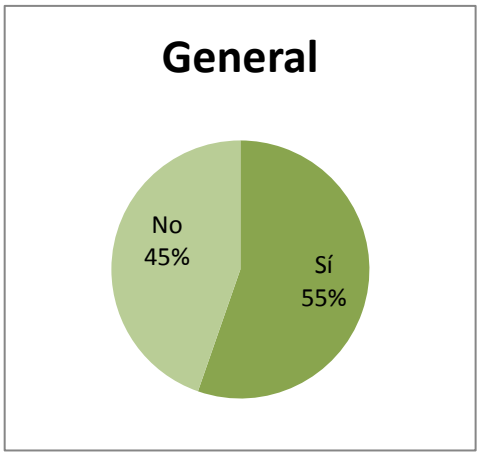
En la pregunta 2 només han contestat aquells qui havien afirmat conèixer la pràctica del Phishing. L'objectiu d'aquesta qüestió era veure si ho sabien realment o tenien una concepció del terme errònia. La resposta correcta és la A, i com podem observar més de la meitat dels enquestats (64%) ha respost bé. Les diferències entre totes tres franges són escasses, cal destacar que en totes predomina la resposta A, en la franja de més de 40 anys concretament és unànime.

Pregunta 3: Creus que tots els hackers duen a terme pràctiques fraudulentes?



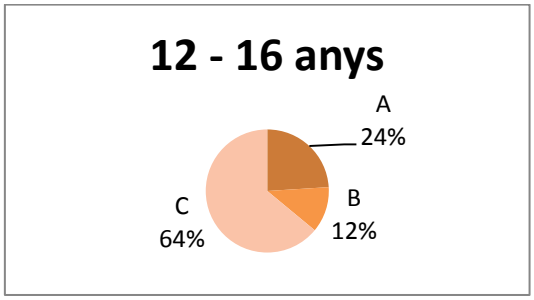


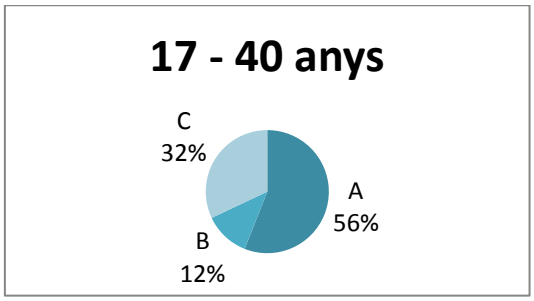


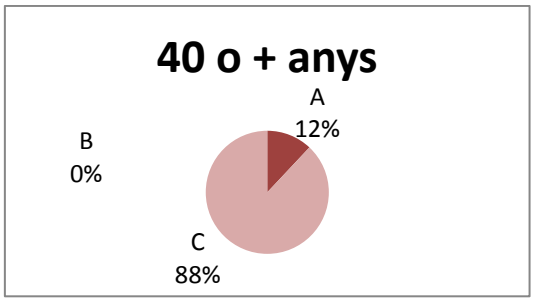


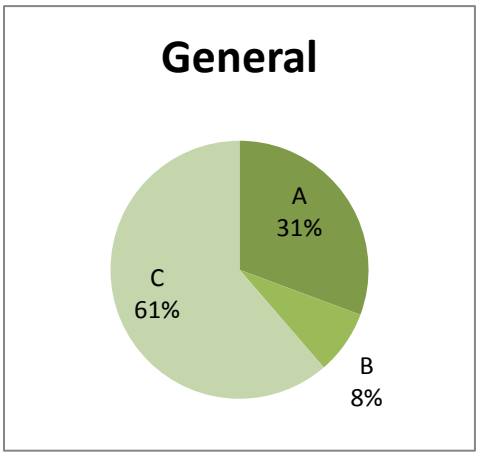
Aquesta pregunta respon a la visió negativa o prejudici que en té la societat sobre la comunitat hacker. Com s'explica en el treball no tots duen a terme pràctiques fraudulentes, i els que ho fan s'anomenen crackers i s'aprofiten de la seva metodologia. En general el prejudici de "tots els hackers són dolents" supera la realitat, només supera la franja del 50% (amb un 74%) el gràfic d'entre 17 i 40 anys. Així doncs es pot observar com en la iniciació informàtica (primer gràfic) encara no és té assolit el concepte "hacker" ni quina és la seva tasca, i en el tercer gràfic (al no tenir una base sobre el tema suficient) ha influït molt la imatge que presenten els mitjans de comunicació, els quals nomenen "hacker" a tot aquell qui programa per fer el mal.

Pregunta 4: I els phishers?



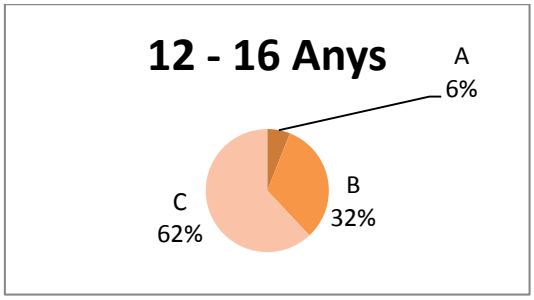


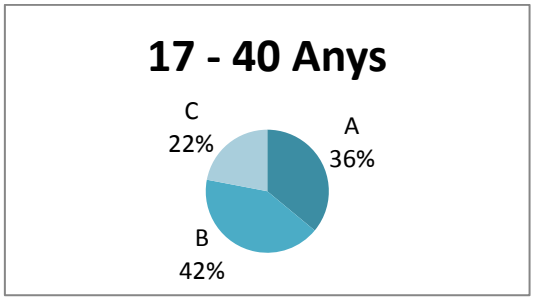


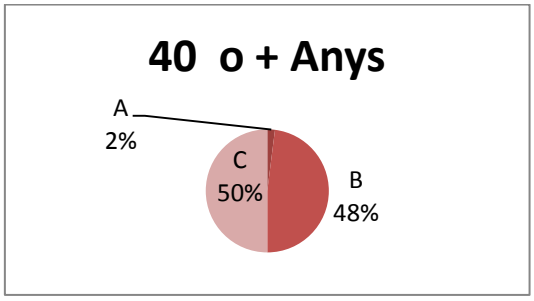


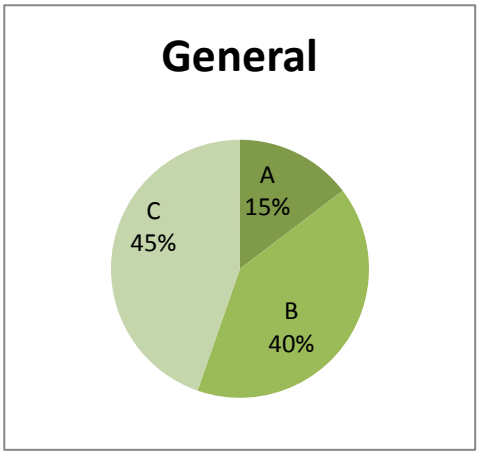
Com era d'esperar després d'analitzar els resultats de la pregunta 1, una gran majoria de gent (61%) no sap si els phishers duen a terme pràctiques fraudulentes, un 31% de la gent afirma que sí, que tots són delinqüents cibernètics, i tan sols un 8% diu que no. En aquest cas la resposta correcta era la A, ja que un phisher SEMPRE realitza tasques il·legals i/o fraus. Si analitzem les tres franges d'edats per separat, predomina altre cop la franja intermèdia en la resposta correcta, en el primer gràfic hi ha diversitat d'opinions i en l'últim una gran majoria no ho sap, però els que afirmen saber-ho proposen la solució correcta.

Pregunta 5: Coneixes o has sentit parlar mai d'algun cas d'atac cibernètic contra la identitat de la persona, empresa, pàgina web... és a dir, un atac de Phishing?







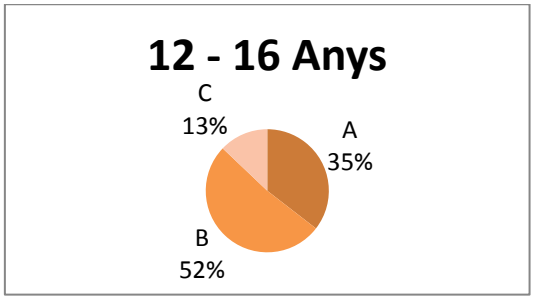


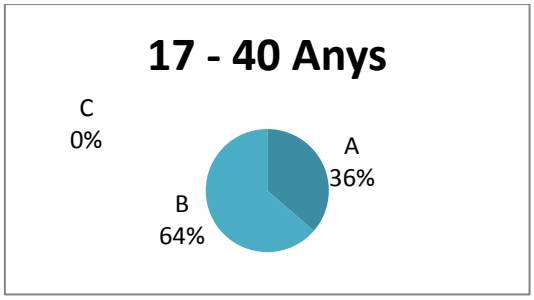
En aquesta qüestió número 5 comença a deixar-se entreveure la definició del terme Phishing, per a que l'enquestat pugui tenir una idea base de que és o en que es basa aquesta pràctica. En general hi ha dos postures que empaten gairebé a percentatge: un 45% de la gent afirma haver sentit parlar d'algun cas d'atac cibernètic d'aquest tipus i un 40% no en coneix ni n'ha sentit parlar mai. En tots tres gràfics els resultats són semblants, però cal destacar en el segon gràfic l'elevat percentatge de gent que afirma haver patit algun atac d'aquests, el qual simbolitza que 2 de cada 10 persones d'entre 17 i 40 anys han sofert algun atac de Phishing, unes dades força alarmants.

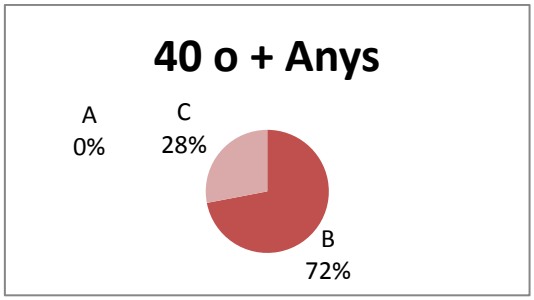
Els casos que proposaven aquells qui havien marcat la A o la B eren majoritàriament sobre xarxes socials i pàgines web, a més d'alguna menció de comptes bancaris.

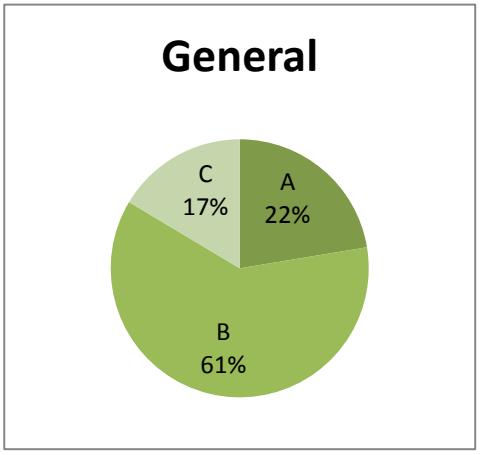
Pregunta 6: Un atac de Phishing pot succeir simplement en la usurpació d'un compte d'alguna xarxa social com Facebook, Instagram, Twitter, etc. Ara doncs, en coneixes algun cas?

* Aquesta pregunta només la responien aquells qui contestaven "No, no en conec cap" a la pregunta 5.









Aquesta pregunta anava dirigida a explicar com pot ocórrer un atac de Phishing a les persones que havien respost que no n'havien sentit parlar mai. Els resultats són força sorprenents ja que més de la meitat d'aquests enquestats restants (el 61%) ha sentit a parlar d'usurpacions de correus o comptes de xarxes socials i fins a un 22% d'aquests n'ha patit. L'única franja d'edat que en aquest cas no ha sofert cap atac és la de més de 40 anys, o bé perquè no en fan un ús tant constant com les generacions més joves, o bé perquè possiblement els phishers veuen el negoci més rentable en la gent més jove. D'aquests quatre gràfics es pot concloure que el percentatge de gent que ha patit atacs d'aquest tipus augmenta si es desconeix el mètode o l'existència de l'amenaça.

Els casos proposats en aquest cas eren únicament comptes de Facebook i Instagram i en dos casos puntuals de Twitter. Són Facebook i Instagram menys segures que les altres xarxes socials? No, però la quantitat d'usuaris diaris és més elevada i per tant hi ha més afectats.

Pregunta 7: Quin mètode o mètodes creus que serien efectius per evitar aquests atacs o almenys posar-hi una mica més de seguretat?

*Exemple: Comprovar sempre que el lloc des d'on Iniciem Sessió o ens Registrem sigui segur.

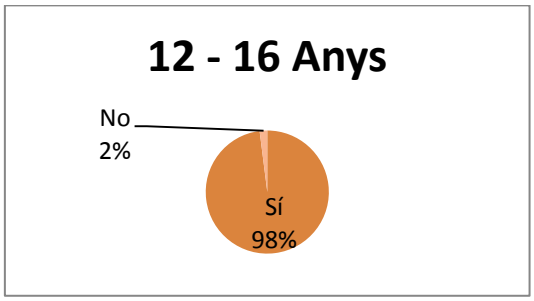
Amb aquesta qüestió buscava, al igual que amb les xerrades a l'alumnat de 1r de ESO, la participació de l'enquestat per a que reflexionés sobre totes aquelles petites recomanacions que hem pogut sentir, aprendre, llegir, deduir inclòs... que vetllen per la seguretat informàtica o de navegació.

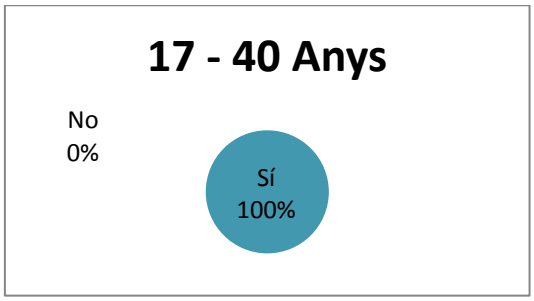
Pràcticament qualsevol persona sap algun mètode, per obvi que sigui, que pugui marcar la diferència entre evitar l'atac o no sense ser-hi conscient. Moltes de les persones que havien marcat "No" a la pregunta número 1: "Coneixes la pràctica del Phishing?" han donat mètodes vàlids per evitar-lo. Llavors, si gairebé tothom sap com evitar o minimitzar aquests atacs, perquè són tan freqüents? El problema s'esdevé en que molts cops no apliquem cap dels mètodes que s'esmenten en les enquestes per senzills que pareguin. Realment no som conscients totalment de l'existència d'aquesta nova amenaça cibernètica que es val de l'enginyeria social per enganyar a la gent i per tant no sembla ser necessari aplicar aquestes recomanacions.

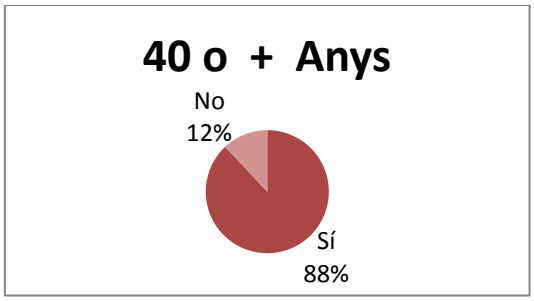
Les propostes més repetides han estat les següents:

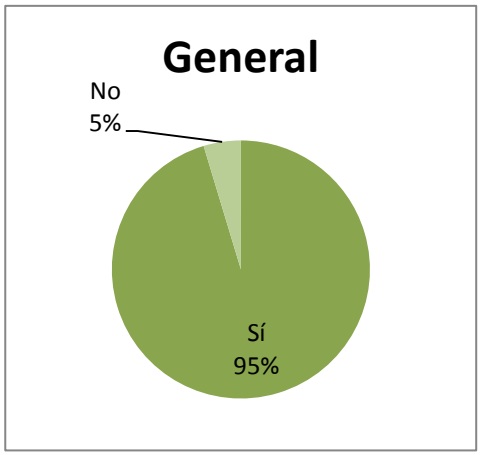
- Comprovar la url de la pàgina web que es visiti.
- Reforçar la seguretat de les contrasenyes.
- No donar informació personal per fiable que paregui la font que la demana.
- Revisar periòdicament els comptes i correus.
- Desconfiar de les fonts desconegudes.
- Etc.

Pregunta 8: Creus necessària o interessant una xerrada informativa sobre el Phishing i com evitar-lo?









La pregunta número 8 suposa l'última qüestió de l'enquesta, la qual estava enfocada a la meva tercera part pràctica, les xerrades informatives sobre el Phishing. L'objectiu era veure si la gent estaria interessada o no en atendre a una d'aquestes xerrades i segons els resultats dur-les a terme o no.

Sorprenentment els resultats són molt positius ja que gairebé tothom (un 95%) pensa que sí, que serien interessants o necessàries. En els enquestats de 12 a 40 anys (els dos primers gràfics), tan sols una persona va marcar que no, per tant, la meva tercera pràctica anirà enfocada per a gent d'aquestes dues franges d'edat.

7. SIMULACIÓ D'UN ATAC PHISHING

En aquest apartat del treball s'han posat en pràctica tots els coneixements adquirits sobre la metodologia Phisher. Consisteix en simular un atac via correu electrònic per obtenir les dades d'una suposada víctima. Per a fer-ho cal haver estudiat tots els apartats anteriors per veure quins són els passos a seguir per finalment reproduir un cas d'atac Phishing simulat.

7.1. Objectiu

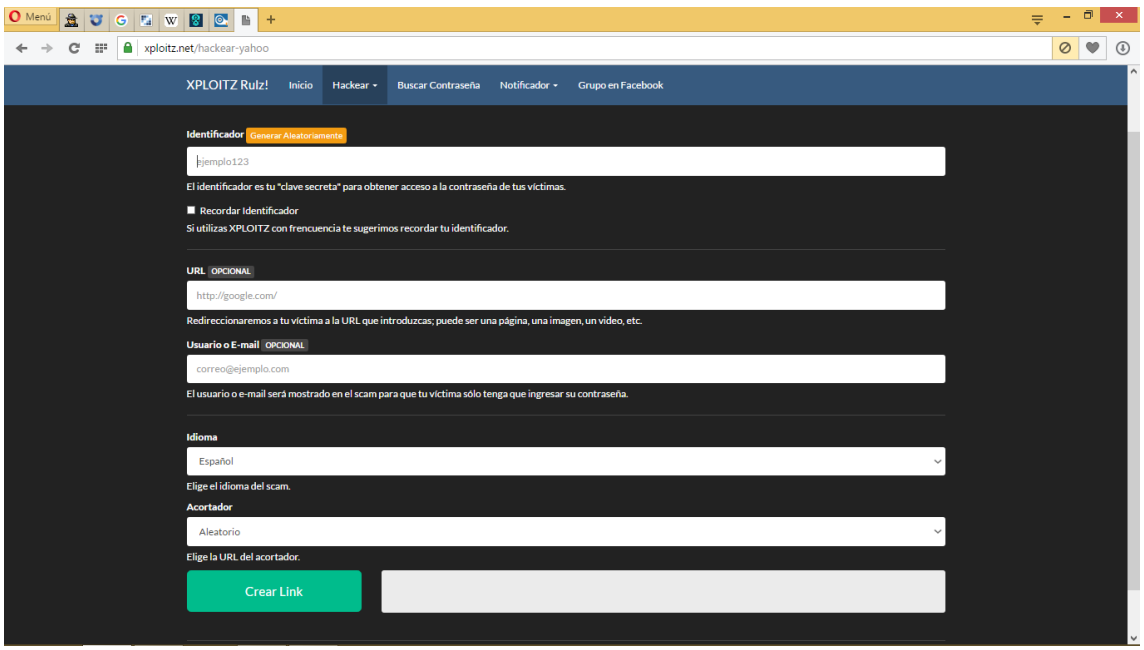
La simulació d'un atac Phishing té com a finalitat posar en pràctica la metodologia Phisher per comprovar quines dificultats suposa, analitzar la resposta de la xarxa social que es vol atacar (si n'hi ha), estudiar el grau de fiabilitat que poden arribar a tenir els correus i el temps que cal dedicar per elaborar aquests atacs.

7.2. Metodologia

El primer pas per a dur a terme una simulació d'un atac d'aquest tipus és escollir per quina via emetrem l'atac. Com hem dit serà via correu electrònic i concretament l'objectiu serà un compte de Yahoo.

En segon lloc hem de triar un sistema de selecció de víctimes. Com que només anem a simular un atac utilitzarem el mètode concret, amb un compte creat per nosaltres: prova.u@yahoo.es amb contrasenya "victimanumero1".

El següent pas és crear un enllaç fals que redirigeixi a una pàgina que sigui aparentment d'inici de sessió de la xarxa escollida, Yahoo en aquest cas. Per a fer-ho, i al no tenir uns coneixements de programació suficients, utilitzarem una pàgina web simple que proposant-li un seguit de dades crearà aquest link i una finestra d'aparença molt acceptable. Aquesta pàgina s'anomena https://xploitz.net



Vista general de les dades que demana la pàgina.

Font: www.xploitz.net

Les dades que es demanen són:

1. **Identificador**

   Es tracta de la clau secreta del phisher per obtenir posteriorment accés a les contrasenyes de les víctimes.

   En el nostre cas el generem aleatòriament i serà: *pdqyH2tWQZEErzYc*

2. **URL**

   Aquí es situa la pàgina web a la qual redireccionem a la víctima en introduir les dades a la pàgina que proporcionem, és a dir, li proporcionem un fals inici de sessió de yahoo i la redireccionem, per exemple, a l'inici de sessió "REAL" per a que la víctima cregui que ha escrit mal la contrasenya, en el segon intent podrà accedir correctament al seu compte i no se n'haurà adonat de l'engany.

   En aquest apartat situem la url següent: https://login.yahoo.com/config/login

3. **Usuari o e-mail**

   Posem el correu de la víctima: prova.u@yahoo.es per a que en entrar des del link ja aparegui posat i només calgui escriure la contrasenya, el qual ho fa més fiable aparentment.

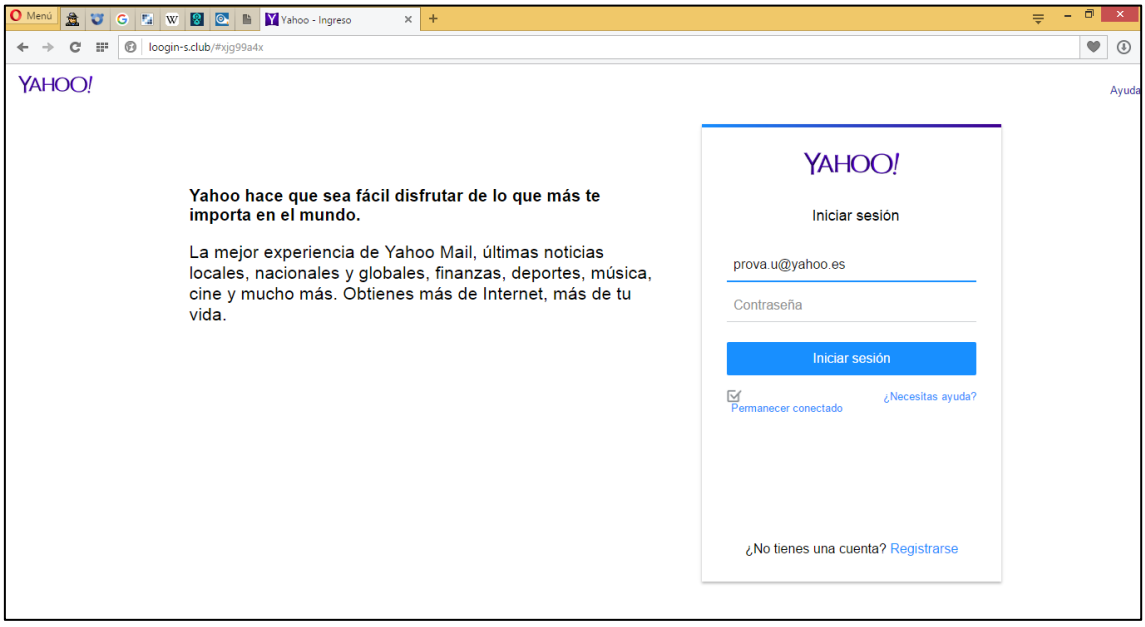
4. **Idioma**

Escrivim si volem que el "scam" o pàgina falsa aparegui en un idioma determinat. En aquest cas esciurem "*Español*"

Per a acabar amb aquest pas premem "Crear link" i seguim les instruccions.

Un cop la pàgina ens proporciona el link següent que hem creat seguint els passos anteriors: http://reeddit.club/#xjg99a4x comprovem que dirigeix a una pàgina aparentment fiable de Yahoo per fer l'atac efectiu.

* En seguir l'enllaç automàticament canvia la url per http://loogin-s.club/#xjg99a4x



Pàgina falsa creada amb xplotiz.net

Font: www.xploitz.net

Pàgina real d'inici de sessió de Yahoo

Font: www.yahoo.es

Com es pot apreciar fàcilment les diferències són mínimes, i si no tenim en ment perfectament la pàgina d'inici real és molt fàcil iniciar sessió des de la primera pàgina i per tant permetre l'atac de Phishing.

Un cop hem comprovat que funciona, el següent pas és enviar un correu convincent a la víctima per a que entri a l'enllaç anterior i inicïi sessió. Per exemple:

"Estimado prova.u,

Recientemente nuestros servicios han experimentado problemas de conectividad y almacenamiento de datos online. Por motivos de seguridad hemos bloqueado su cuenta. Para desbloquearla inicie sesión desde: http://reeddit.club/#xjg99a4x y accede a tu perfil. Disculpe las molestias.

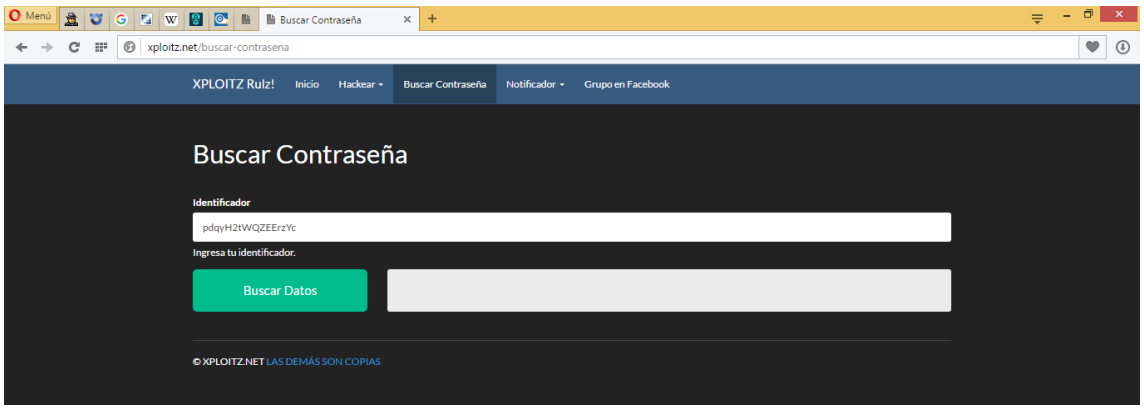
Atte. Yahoo España"

Un cop enviat el pas següent es esperar a que la víctima "mossegui l'ham" i ens lliure les dades. En aquest cas nosaltres mateixos obrim aquest enllaç i escrivim la contrasenya que havíem escollit: victimanumero1

En efectuar-ho ens redirigeix a la pàgina real d'inici de sessió de Yahoo tal i com havíem triat, i aquest cop ja podríem entrar amb normalitat.

És el moment de recollir les dades: tornem a la pàgina de Xploitz i copiem el segon link proporcionat després del "scam". Seria el següent: http://xploitz.net/b/pdqyH2tWQZEErzYc i ens apuntem el nostre identificador aleatori creat anteriorment. Un cop copiat, seguim l'enllaç.

Ens apareix una finestra com aquesta:



Obtenció de les dades

Font: www.xploitz.net

Hi situem l'identificador i premem "Buscar Datos" i seguim les instruccions.

Finalment la pàgina web ens ofereix la informació obtinguda a partir de la pàgina falsa de Yahoo que hem creat, en aquest cas ens proporcionaria la contrasenya de l'anterior correu electrònic.

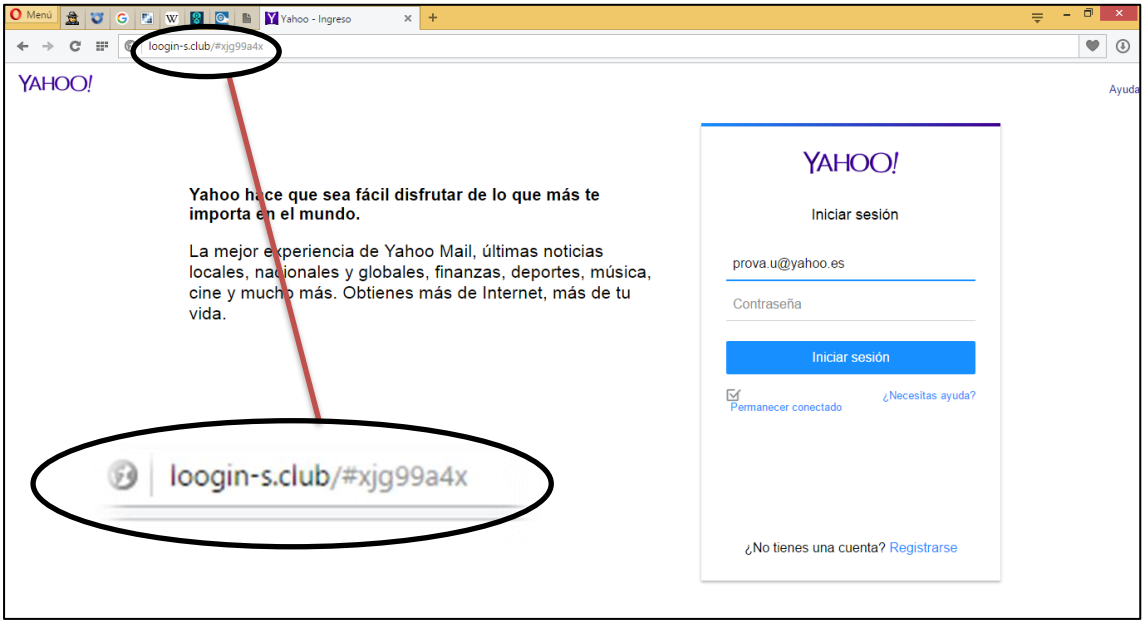
7.3. Conclusions

Al llarg d'aquesta pràctica he pogut observar com, amb una mica d'experiència amb la pàgina i les víctimes escollides per endavant, amb un temps de 2-5 minuts pots arribar a tenir creat un "scam" o pàgina falsa totalment fiable amb la qual obtenir-ne les contrasenyes dels comptes desitjats. Això suposa una gran facilitat per al phisher que l'únic que ha de fer és esperar i comprovar els resultats.

En aquest cas, jo no tinc gairebé cap coneixement de programació i he tingut que recórrer a una pàgina web inundada de publicitat i d'una fiabilitat baixíssima. A més, he de dir que en l'última realització d'aquesta simulació no n'he obtingut la contrasenya com esperava, però sí va resultar efectiu quan ho vaig provar per primera vegada al setembre de 2016. Això és deu a que aquestes xarxes socials s'actualitzen diàriament per vetllar per la seguretat dels seus usuaris i protegir-se d'atacs que vulnerin els seus serveis.

El fet preocupants és, que si jo, sense tenir coneixement de programació he pogut trobar tan fàcilment aquesta pàgina i en un primer moment utilitzar-la (amb fins totalment experimentals) amb resultats efectius, un phisher expert, un cracker professional... es poden arribar a aturar? I si no és així, fins a quin punt estem segurs?

Amb aquesta reflexió apareix la importància de conèixer alguns dels consells bàsics anti-phishing esmentats en un apartat anterior. En la meva simulació, la clau per veure que es tracta d'un enllaç fals és analitzar l'URL:



En aquest cas és molt fàcil de detectar que es tracta d'una url falsa i que no és correspon, però en el cas d'un atac professional és possible que només es diferenciessin per una lletra, un número o fins i tot un símbol, i cal estar molt atent.

Si apliquem el principi fonamental per evitar aquests atacs: EL SENTIT COMÚ, des d'un principi no obrirem l'enllaç proporcionat sinó que escriurem nosaltres mateixos la direcció d'inici de sessió en el buscador, evitant d'aquesta manera un possible atac.

8. XERRADES PREVENTIVES

Aquesta és la pràctica de més transcendència del treball, ja que posa a prova tots els coneixements obtinguts per assabentar un grup de persones dels perills que suposa el Phishing i intentar ensenyar-los a defensar-se. És potser la part que culmina amb l'objectiu principal del treball, que al cap i a la fi és compartir uns consells o nocions bàsiques com a mètode de protecció d'aquest tipus d'atacs.

8.1. Objectius

- Explicar en què consisteix el Phishing.
- Ensenyar a partir de la investigació feta com defensar-se dels atacs de Phishing.
- Assabentar de la gran popularització del mètode i la gravetat dels atacs.
- Conscienciar a futurs internautes de la importància d'una navegació segura.

8.2. Metodologia

Per a dur a terme les xerrades preventives sobre el Phishing he utilitzat un format Power Point com a suport per dur a terme les explicacions (Annex 1).

Vaig escollir fer-la als alumnes de 1r d'ESO per un motiu: tots ells acaben d'entrar a l'institut, la segona etapa de l'educació on, avui per avui, l'eina fonamental d'estudi que s'utilitza és l'ordinador. Aquest any, per a molts d'ells, comença un camí d'experimentació, navegació, entreteniment... amb la informàtica, un món gairebé infinit que cal entrar-hi amb precaució, ja que conté també molts perills. Així doncs, és una gran oportunitat poder compartir una sèrie de consells bàsics amb aquests alumnes per a que comencin aquesta etapa amb la base suficient de coneixement sobre seguretat i les possibles amenaces que cada cop són més presents a la xarxa.

És una opció per evitar aprendre a defensar-se del Phishing a partir de l'experiència, i crec que el millor moment per conèixer aquests consells és en aquest període d'iniciació informàtica en el que acaben d'entrar els alumnes de 1r.

Per a dur a terme les xerrades, a part de l'elaboració del Power Point necessitava també el permís dels seus tutors Amada i Roman, als quals els agraeixo la seva col·laboració i ajut, i determinar uns horaris. La duració d'aquestes era d'una hora, per tant he emprat un divendres de 2 a 3 h. per a 1r A i un dilluns de 2 a 3 h. per a 1r B.

Les xerrades consten d'una combinació d'explicacions i compartir els coneixements estudiats amb el debat de tota l'aula, ja que per assolir bé els conceptes és necessària la participació contínua de l'alumnat i a més permet mantenir l'interès durant el transcurs de tota la xerrada.

Durant aquesta he anat explicant, preguntant i responen a tots els dubtes que presentaven els alumnes, mentre ensenyava què volia transmetre'ls i com protegir-se d'allò que els havia explicat, del Phishing. Mentre, una companya de classe de 2n de Batxillerat feia alguna fotografia i gravava en vídeo (Annex 2) algun tram de l'exposició. Per a les gravacions i les fotos es tenia en compte que l'alumnat de 1r no mostrés la cara, per no comprometre la seva imatge en el cas que algú no hi estès d'acord (les fotografies que apareixen al treball tenen el consentiment de l'alumne en particular que mostra la cara).

Un cop acabada, hem passat al torn final de preguntes, i posteriorment a aquest he repartit uns qüestionaris per a analitzar si havia aconseguit el meu propòsit.

8.3. Resultats dels qüestionaris

Qüestionari alumnat 1r d'ESO		
Número d'assistents	60 alumnes + 2 professors	
T'ha agradat la xerrada?	Sí 62	No 0
Trobes interessant la temàtica?	Sí 62	No 0

Has aprés alguna cosa que no sabies?	Sí 56	No 6
Posaràs en pràctica alguna cosa apresa?	Sí 50	No 12
Puntua de l'1 al 10 la sessió	**Mitjana: 9,15**	

8.4. Conclusions

Després d'analitzar els resultats obtinguts amb els qüestionaris anònims, és molt satisfactori veure com la tasca a dur a terme ha sortit de la millor manera possible, a tots els assistents els interessava el tema i els ha agradat la xerrada. Interessava també comprovar si allò que s'estava explicant era nou per als alumnes, la qual cosa no és positiva ja que denota poca consciència dels perills que presenta la xarxa. El que realment aprova la xerrada és que 50 de les 62 persones afirmen que utilitzaran algun dels consells compartits en la sessió, això possibilitarà una navegació més segura i un increment de l'evasió de les possibles amenaces de Phishing.

Finalment cal esmentar que la nota mitja que han puntuat sobre la sessió els alumnes i els dos professors assistents és de 9,15.

L'objectiu de les xerrades era explicar, ensenyar i compartir idees i coneixements amb l'alumnat de 1r d'ESO, però sorprenentment han acabat per ensenyar-me a mi. Durant el transcurs de les dues sessions he gaudit de l'oportunitat de transmetre una informació sobre el món que més m'apassiona, he entès la veritable presència d'aquest món en la vida de qualsevol de nosaltres i com pot afectar a cada individu segons l'ús que en fa. Els alumnes, amb les seves aportacions i preguntes m'han obert un ventall de reflexions que han contribuït en l'elaboració d'una conclusió final per a aquestes dues xerrades: Combatre el Phishing individualment, amb els consells d'un col·lectiu. És a dir, gràcies a les anècdotes que em contaven, les qüestions que em formulaven o els dubtes que els anaven sorgint he comprés que evitar els atacs produïts mitjançant la enginyeria social es basa en compartir i adoptar consells d'altres internautes i crear els teus propis. No existeix un mètode infal·lible per evitar-los, però amb la difusió d'unes nocions bàsiques de protecció i navegació segura, qualsevol usuari reduirà notablement les probabilitats de possibles atacs de Phishing.

9. CONCLUSIONS

El Phishing en definitiva, és tan sols un mètode més que utilitzen els ciberdelinqüents per lucrar-se de manera il·legal robant dades de qualsevol usuari, empresa, pàgina web, organització... Per extreure unes conclusions adequades sobre la recerca i investigació d'aquesta amenaça, és necessari que ens situem al principi del camí, recordar què és el Phishing i per què és tant important.

Aquest tipus de ciberdelicte es fonamenta amb l'estudi de tècniques d'enginyeria social basades en la manipulació d'unes possibles víctimes per dir o fer quelcom que el Phisher o Enginyer Social demana. Aquesta pràctica sovint es confon amb la tasca d'un Hacker, que a causa d'un prejudici social erroni molt estès pels mitjans de comunicació, simbolitza la imatge dels pirates informàtics. Definitivament no tenen res a veure. Un Hacker o Furoner és una persona apassionada per la informàtica, que té un gran coneixement de les xarxes i els sistemes informàtics i un viu interès per a explorar-ne les característiques i per a posar a prova les seves habilitats en aquest àmbit. N'existeixen de tres tipus: Black Hats, White Hats i Grey Hats. Els Phishers, en canvi, formen part del conjunt real de pirates informàtics o també anomenat Crackers. La diferència entre un Cracker habitual i un Enginyer Social rau en la manera d'obtenir la informació. Els primers utilitzen gestes o tècniques brusques per violar la seguretat d'un sistema informàtic. En el segon cas, s'enganya la víctima per que sigui ella mateixa qui lliure les dades inconscientment.

Existeixen diverses maneres de dur a terme un Phishing (atac), les quals depenen de dos grans factors: en primer lloc s'ha de tenir en compte el tipus d'informació que es desitja o es vol estafar a les víctimes, com podrien ser dades personals, informació financera o credencials d'accés, el segon factor que determinarà el tipus de Phishing fa referència a quin tipus de víctimes anirà dirigit l'atac; es poden escollir les víctimes aleatòriament, per franges d'edat, sexe... o en alguns casos en particular s'escull un determinat nombre de víctimes reduït, les quals han estat estudiades anteriorment.

Depenent de les premisses escollides, l'Enginyer Social actuarà utilitzant un mètode de propagació o un altre. N'existeixen de diversos tipus: mitjançant les xarxes socials, per SMS / MMS, amb en enquestes telefòniques... però el més popular i utilitzat és l'atac via correu electrònic, molts cops acompanyat d'una infecció de malware destinat a estendre's per l'ordinador de la víctima.

La figura del Phisher regeix sempre dos característiques fonamentals: alts coneixements sobre programació i un nivell elevat de tècniques de persuasió o

enginyeria social. En moltes ocasions, però, els atacs es duen a terme per empreses il·legals de Phishing que es dediquen a estendre aquesta amenaça massivament.

Un cop hem arribat en aquest punt intermedi de la recerca, on ja coneixem la pràctica i una gran quantitat de característiques d'ella, el següent pas es plantejar-nos com es duu a terme, és a dir, com es posa en pràctica aquest tipus d'atacs per posteriorment saber evitar-los. Així doncs necessitem conèixer la metodologia Phisher.

El primer pas és determinar el tipus d'atac: quina informació es vol obtenir i com s'escolliran les víctimes. A partir d'aquests dos factors és necessari triar un mètode de propagació adient amb una eficiència més elevada segons les característiques que ha de tenir l'atac. Finalment, després d'emprar el mètode escollit i esperar els resultats s'utilitzen mètodes per netejar possibles pistes que puguin desemmascarar el ciberdelinqüent: ocultació d'IP, VPN i geolocalitzadors i l'ús de la moneda virtual o Bitcoin per dur a terme les transaccions. En el cas d'un atac via correu electrònic, el pas d'emprar aquest mitjà de propagació consisteix en la falsificació d'un ens de confiança i creació d'un correu convincent, aparentment fiable i concís, la distribució del correu segons la selecció de víctimes que s'ha fet i l'actuació posterior en cas que les víctimes hagin sigut manipulades eficientment (mitjançant scams, cryptolockers...).

A partir del moment que coneixem com actua el Phisher, podem començar a concloure com fer-li front als seus atacs, utilitzant tècniques anti-phishing. El primer pas és identificar l'amenaça utilitzant els deu consells proposats en "el decàleg de l'anti-Phishing" que hem elaborat en el treball o d'altres. Totes aquestes recomanacions, però, sempre aniran de la mà del mètode més efectiu contra l'Enginyeria Social: el sentit comú. Posteriorment a la identificació de l'amenaça, es procedeix a aplicar una resposta, o bé ignorar i eliminar-la, o combatre-la mitjançant la resposta organitzativa, tècnica i finalment judicial. La teoria és clara i posada a la pràctica resulta molt efectiva, però, fins a quin punt la societat n'és conscient d'aquesta pràctica fraudulenta tan present a la xarxa avui en dia? El problema s'esdevé en aquest tram del camí per combatre el Phishing, l'usuari, generalment desconeix l'amenaça i per tant no sap protegir-se i aquest desconeixement s'intensifica en les franges d'edat compreses entre 12-16 i més de 40 anys. És possible que ensenyar o compartir amb la gent de més de 40 anys com combatre el Phishing sigui una tasca generalment innecessària, ja que l'ús d'aquestes persones de la xarxa és majoritàriament més moderat, cautelós, limitat, responsable... i això suposa un minvament notable del risc. En el cas de la primera franja (de 12 a 16 anys) la navegació és molt més abundant, inexperta, ràpida, curiosa... la qual cosa augmenta considerablement el risc d'un possible atac de

Phishing efectiu. Per aquest motiu, la necessitat d'ensenyar a aquest conjunt l'existència de l'amenaça i els mètodes de defensa d'aquesta i possiblement d'altres pràctiques perilloses que circulen per Internet suposa una gran oportunitat per començar amb bon peu el seu viatge per l'era de la informació, per l'era digital. Aquest és el motiu principal de les xerrades preventives sobre l'Enginyeria Social aplicada a la informàtica dutes a terme a l'alumnat de 1r d'ESO.

L'elaboració d'un atac de Phishing és relativament tan senzill com evitar-lo, sense tenir pràcticament cap coneixement de programació s'ha pogut aconseguir simular un exemple d'aquests ciberatacs amb uns resultats molt propers a la captació de les dades la víctima, però evitat pels sistemes de seguretat de la xarxa social Yahoo. És fàcilment deduïble que els Phishers professionals o les empreses que duen a terme aquests fraus gaudeixen d'uns estudis o aprenentatges, així doncs, dur a terme un atac no suposa cap dificultat per a aquest tipus de ciberdelinqüents. Alhora, identificar un atac no requereix d'un sistema de seguretat molt sofisticat, sinó de la consciència de la seva existència i els "tips" bàsics per adonar-se de l'engany. Com bé afirma Kevin Mitnick, per molts programes o firewalls de protecció que tinguem, mai no són garantia d'una total seguretat, al cap i a la fi la seguretat no és un producte, sinó un procés. Un procés que evoluciona gairebé al mateix ritme que la ciberdelinqüència, un fet que resulta força preocupant.

L'usuari és vulnerable, i ho és més si no sap com defensar-se. La clau per a la seguretat informàtica vers l'Enginyeria Social no rau en els antivirus més cars o els softwares més complexos, sinó en aplicar el sentit comú, en compartir experiències perquè un tercer no passi pel mateix, en ser conscients dels perills d'Internet, però també dels abundants beneficis que proporciona si se'n fa un bon ús... en definitiva, la base d'una bona protecció contra el Phishing ha de ser construïda per i per a l'usuari (l'usuari aprèn d'un altre i més tard ho comparteix amb un tercer).

És possible l'eradicació total del Phishing, doncs? Creure en la desaparició d'algun tipus de cibercelicte d'aquest tipus avui dia podria considerar-se una opinió visionària, i més sabent que aquest anirà evolucionant a mesura que les tècniques d'anti-Phishing ho facin. Això no hauria de suposar cap motiu d'alarma, al contrari, hauria d'esdevenir un impuls per ensenyar a combatre'l i aconseguir d'aquesta manera disminuir la seva eficiència i, en un futur, considerar-lo tan sols: un perill més de l'era digital.

9.1. Si tornes a començar...

Què canviaria si tornes a començar aquest treball? És una pregunta que m'ha fet reflexionar molt, i puc afirmar que canviar potser només canviaria els meus horaris per realitzar el treball, els quals han estat de moltes tardes però estones breus i al final el temps se m'ha tirat una mica a sobre. Però més que canviar, afegiria. El cas és que m'ha apassionat dur a terme aquesta recerca i sentia que volia saber més, però segurament mai acabaries satisfet del tot. M'hagués agradat que la simulació de l'atac hagués resultat, però degut a la meva inexperiència i desconeixement dels softwares utilitzats pels phishers era força fàcil de predir que fallés. En definitiva estic satisfet amb els resultats, i si tornés a començar escolliria el mateix tema sens dubte, em replantejaria els horaris i gaudiria novament d'aquesta investigació.

9.2. Què he aprés?

Durant tota aquesta investigació m'he n'he adonat que per molt temps que s'hagi invertit en la realització del treball, no és equiparable a la quantitat de nous coneixements i experiència que he pogut obtenir.

Primerament he conegut la pràctica del Phishing, aquell mètode fraudulent que fa cosa d'un any va despertar en mi gran curiositat i encara ara la segueixo sentint. A conseqüència d'entendre en què consisteixen els atacs d'Enginyeria Social he pogut determinar com evitar-los, per poder, en un futur, compartir aquestes tècniques amb d'altres usuaris.

A més, no tan sols he adquirit coneixements sobre el tema tractat, sinó que he reforçat les meves tècniques de recerca i síntesi, així com d'expressió, anàlisi...

9.3. Què m'ha agradat més/menys?

El que m'ha agradat més sens dubte ha estat dur a terme les xerrades a l'alumnat de 1r d'ESO i la repercussió positiva que han tingut, veure com alguns d'ells es quedaven a preguntar-me dubtes, que dies més tard venien a consultar-me inquietuds o a compartir anècdotes... recordant-me a, no fa gaires anys, quan jo començava a sentir interès per l'immens món de la informàtica.

D'altra banda, el que m'ha agradat menys, com en quasi tots els treballs, ha estat fer les citacions bibliogràfiques, pot semblar una idea una mica ximple, però sempre se m'han resistit, em sembla una tasca si més no avorrida i més difícil de trobar la informació necessària del que aparenta.

9.4. Quines coses ens han quedat pendents?

En aquest sentit estic força satisfet per haver resolt tots els objectius plantejats al principi del treball amb més o menys eficiència, tot i que sempre hi ha coses per millorar. Una d'aquestes, la qual m'ha desanimat una mica, és la simulació d'un atac de Phishing que no ha resultat del tot. D'altra banda, reforça la teoria de que les xarxes socials treballen constantment en la millora de la seva seguretat, la qual cosa implica que potser el mètode que estava utilitzant ja havia estat bloquejat.

10. AGRAÏMENTS

Finalment, m'agradaria agrair la col·laboració de tots aquells que van respondre amablement les enquestes sobre el Phishing, als professors de 1r d'ESO i els seus alumnes per deixar-me dur a terme les xerrades i per ser un públic molt participatiu, també a les companyes Júlia Querol i Sorina Teleki per enregistrar en vídeo i fotografiar les xerrades. També vull agrair la informació lliurada pels informàtics Raúl Garcia i Josep Subirats, que em van explicar el funcionament dels atacs, el mercat del Bitcoin i altres dades rellevants del treball. Per acabar, dono gràcies als meus pares per haver-se preocupat perquè hi posés tota la dedicació i concentració possible i, en especial, al meu tutor Ricard Reverter Forcadell qui s'ha dedicat a assessorar el meu treball, m'ha ajudat, donat idees, corregit i fins i tot compartit opinions i coneixements sobre el tema.

Moltes gràcies a tots aquells qui heu posat el vostre granet d'arena en aquest treball, i moltes gràcies a tu, per haver-lo llegit.

11. BIBLIOGRAFIA I WEBGRAFIA

Per a dur a terme la recerca d'informació he utilitzat les següents fonts bibliogràfiques o digitals:

11.1. Bibliografia

Mitnick, K. and Simon, W. (2002). *The art of deception*. 1st ed. Indianapolis, Ind.: Wiley Pub.

Hadnagy, C. (2011). *Social engineering*. 1st ed. Hoboken, N.J.: Wiley.

11.2. Webgrafia

Seguridad en Sistemas y Técnicas de Hacking. TheHackerWay (THW). (2017). *¿Qué es el Hacking?*. [online] Disponible a: https://thehackerway.com/about/ [Última visita 14 Jan. 2017].

The Economic Times. (2017). *Definition of 'Hacking' - The Economic Times*. [online] Disponible a: http://economictimes.indiatimes.com/definition/hacking [Última visita 29 Juny. 2016].

Díaz, M., Arroyo, M., Díaz, M., Díaz, M., Arroyo, M., Camacho, M., Arroyo, M., Camacho, M., Verdés, F. and Verdés, F. (2017). *Hacking Ético*. [online] Hacking Ético. Disponible a: https://hacking-etico.com [Última visita 3 Juliol. 2016].

G3ek Army. (2017). *Origen de la palabra Hacker - G3ek Army*. [online] Disponible a: http://g3ekarmy.com/origen-de-la-palabra-hacker/ [Última visita 4 Juliol 2016].

Rivero, M. (2017). *¿Qué es el Phishing?* | *InfoSpyware*. [online] Infospyware.com. Disponible a: https://www.infospyware.com/articulos/que-es-el-phishing/ [Última visita 16 Agost 2016].

Goo.gl. (2017). *Phishing | Informacion | Evolucion | Protección-Información sobre Seguridad-Panda Security*. [online] Disponible a: https://goo.gl/ABF6EI [Última visita 16 Agost 2016].

Ca.wikipedia.org. (2017). *Pesca (informàtica)*. [online] Disponible a: https://ca.wikipedia.org/wiki/Pesca_(informàtica) [Última visita 1 Setembre 2016].

Anòn., (2017). [online] Disponible a: https://goo.gl/d0xeVB [Última visita 16 Setembre 2016].

Es.wikipedia.org. (2017). *Servidor proxy*. [online] Disponible a: https://es.wikipedia.org/wiki/Servidor_proxy [Última visita 21 Desembre 2016].

Llorca, Á. (2017). *VPN: ¿qué es y para qué sirve? - Nobbot*. [online] Nobbot. Disponible a: http://www.nobbot.com/tecnologia/mi-conexion/vpn [Última visita 23 Desembre 2016].

País, E. (2017). *¿Qué es el bitcoin? La moneda que controlan todos y nadie a la vez*. [online] EL PAÍS. Disponible a: https://goo.gl/AgkyZG [Última visita 27 Desembre 2016].

El Confidencial. (2017). *Incluir mayúsculas y números no hace tu contraseña más segura. Noticias de Tecnología*. [online] Disponible a: https://goo.gl/9n2CHs [Última visita 27 Desembre 2016].

Xploitz.net. (2017). *XPLOITZ*. [online] Disponible a: https://xploitz.net [Última visita 29 Desembre 2016].

Edu365.com. (2017). *Treball de recerca*. [online] Disponible a: http://www.edu365.com/batxillerat/comfer/recerca/ [Última visita 4 Gener 2017].

Es.wikipedia.org. (2017). *Ingeniería social (seguridad informática)*. [online] Disponible a: https://es.wikipedia.org/wiki/Ingeniería_social_(seguridad_informática) [Última visita 7 Gener 2017].

Goo.gl. (2017). *Dos casos reales de robo de dinero con suplantación de identidad de ayer mismo*. [online] Disponible a: https://goo.gl/wqeSgW [Última visita 7 Gener 2017].

Interior.gob. (2017). *Convenio de cibercminalidad de Budapest*. [online] Disponible a: http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815 [Última visita 9 Gener 2017].

Goo.gl. (2017). *Phishing | Informacion | Evolucion | Protección-Información sobre Seguridad-Panda Security*. [online] Disponible a: https://goo.gl/fE0cBo [Última visita 9 Gener 2017].

CANO, R. (2017). *Kevin Mitnick: "En mi época, 'hackeábamos' por diversión. Hoy, por dinero"*. [online] EL PAÍS. Disponible a: http://tecnologia.elpais.com/tecnologia/2010/01/27/ actualidad/1264586463_850215.html [Última visita 14 Gener 2017].

Ingeniería Social. (2017). *Ingeniería Social I Consultoria i Auditoria en RSC*. [online] Disponible a: http://ingenieriasocial.es/ca/ [Última visita 14 Gener 2017].

TheFreeDictionary.com. (2017). *Phisher*. [online] Disponible a: http://www.thefreedictionary.com/Phisher [Última visita 14 Gener 2017].

Rae.es. (2017). *Real Academia Española*. [online] Disponible a: http://www.rae.es

Dlc.iec.cat. (2017). *Institut d'Estudis Catalans - Diec2*. [online] Disponible a: http://dlc.iec.cat

Wordreference.com. (2017). *Diccionarios de Español, Ingles, Francés, Portugués - WordReference.com*. [online] Disponible a: http://www.wordreference.com/es/

Diccionaris.cat. (2017). *Diccionaris en català: diccionari català-castellà català-anglès català-francès sinònims*. [online] Disponible a: http://diccionaris.cat

Goo.gl. (2017). *Siete consejos para evitar ataques de phishing en tu cuenta de Facebook | Kaspersky Lab Mexico*. [online] Disponible a: https://goo.gl/PD7sdq [Última visita 14 Gener 2017].

Goo.gl. (2017). *Seis consejos para evitar los ataques de 'phishing'*. [online] Disponible a: https://goo.gl/x6R1zT [Última visita 14 Gener 2017].

YouTube. (2017). *Tutorial de Hacking:Ataque Phishing, que es y como protegerse*. [online] Disponible a: https://www.youtube.com/watch?v=AcFG4zyNIRM [Última visita 14 Gener 2017].

YouTube. (2017). *Como hackear redes sociales e emails FACEBOOK,TWITTER,INSTAGRAM,SNAPCHAT,GMAIL,HOTMAIL,YAHOO*. [online] Disponible a: https://www.youtube.com/watch?v=R_X-j5-wkG0 [Última visita 14 Gener 2017].