Phishing

Nocions bàsiques i consells.

Guia per a combatre'l

[ÍNDICE]

Continguts

1 QUÈ ÉS EL *PHISHING*?

El *phishing*, en català hauríem de dir pesca (encara que està molt acceptat el terme en anglès) és un frau de suplantació d'identitat que sol fer-se per correu electrònic, encara que també per missatgeria instantània i fins i tot per telèfon, per obtenir dades de targetes de crèdit, dades bancàries o altres tipus d'informació d'interès.

En aquests missatges els ciberdelinqüents es fan passar per una persona o empresa coneguda i de confiança i amb tota mena d'arguments normalment relacionats amb la seguretat - la nostra seguretat sobretot - volen fer-nos "mossegar l'ham" per a què introduïm les nostres dades en una pàgina web que ells ens indiquen i així poder-se fer amb elles.

I per què les volen?

Per robar-nos, ja siguin diners dels nostres comptes bancaris i targetes o fent compres al nostre càrrec, per cometre estafes i altres delictes suplantant la nostra identitat, per vendre'ls a tercers que també podran cometre delictes... Vaja, per a res de bo. :-(

[ÍNDICE]

2 TIPUS DE *PHISHING*

Hi ha molts tipus d'atacs de *phishing* però tots tenen en comú l'ús d'un pretext fraudulent (problemes de caràcter tècnic, deteccions de fraus recents, noves recomanacions de seguretat, canvis en la política de seguretat de l'entitat...) per adquirir dades valuoses (dades personals, bancàries, credencials d'accés a serveis de correu, a comerços en línia, etc.).

La majoria dels mètodes de *phishing* utilitzen la manipulació en el disseny del correu electrònic per aconseguir fer-se passar per un tercer (organització, empresa, banc...) i normalment que un enllaç sembli una ruta legítima d'aquesta organització per la qual es fa passar l'impostor, perquè confiem i introduïm les dades que ens sol·liciten.

Les **URLs manipulades, o l'ús de subdominis**, són trucs comunament usats; per exemple en aquesta URL: http://www.nomdelteubanc.com/exemple, en què el text mostrat a la pantalla no correspon amb l'adreça real a què condueix.

O de vegades l'atacant utilitza contra la víctima **el codi de programa del banc o servei pel qual es fa passar.** Aquest tipus d'atac resulta particularment problemàtic, ja que dirigeix

l'usuari a iniciar sessió a la pàgina del banc o servei, on la URL i els certificats de seguretat semblen correctes. En aquest mètode d'atac (conegut com ***Cross Site Scripting***) els usuaris reben un missatge dient que han de “verificar” els comptes, seguit per un enllaç que sembla ser la pàgina web autèntica; en realitat, l'enllaç està modificat per fer aquest atac, a més és molt difícil detectar si no es tenen els coneixements necessaris.

També tenim el que es coneix com a ***Spear phishing*****, que són atacs dirigits a objectius concrets**. En general la majoria de campanyes de *phishing* envien correus electrònics massius al major nombre possible de persones, en canvi aquest tipus de *phishing* va dirigit a una persona o organització específica, sovint amb contingut personalitzat per a la víctima o víctimes. Això implica que els ciberdelinqüents necessiten un reconeixement previ per descobrir noms, càrrecs, adreces de correu electrònic i semblants. Els ciberdelinqüents busquen a Internet tota aquesta informació per crear un correu electrònic creïble. Per això cal anar amb compte amb la informació que fem pública a Internet (xarxes socials, webs...).

A l'anomenat "***phishing*** **de clonació**" el que fan és una còpia d'un **correu electrònic legítim** enviat anteriorment que conté un enllaç o un fitxer adjunt, i el ciberdelinqüent substitueix els enllaços o fitxers adjunts amb contingut maliciós disfressat per fer-se passar per l'autèntic. Els usuaris desprevinguts fan clic a l'enllaç o obren l'adjunt perquè creuen que és de confiança i amb això poden prendre el control dels seus sistemes, robar dades, etc, que

[ÍNDICE]

després els serviran per falsificar la identitat de la víctima per fer-se passar per un remitent de confiança davant d'altres víctimes de la mateixa organització.

I no podem deixar de comentar les curioses i famoses estafes conegudes com a **"Estafes nigerianes"**. Qui no ha rebut mai un correu electrònic d'algú que afirma ser un príncep nigerià, o empresari d'algun país africà, que disposa de molts diners però necessita ajuda per poder transferir-lo des del país en qüestió a un altre país més segur, i en demana un compte bancari on transferir aquests diners a canvi d'una important comissió. Al llarg dels anys han aparegut multitud de variants de l'estafa original, i encara que sembli increïble, hi ha persones que encara avui continuen caient al parany.

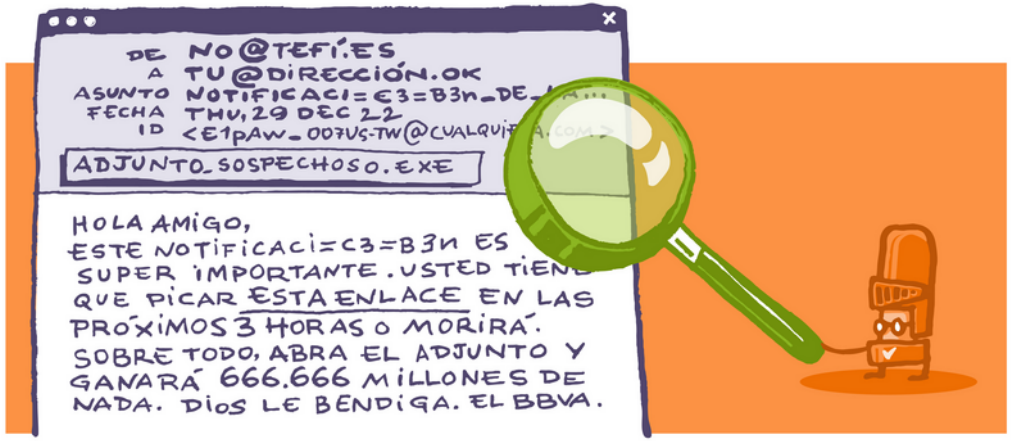
Comentar també que lamentablement el *phishing* abasta més que només Internet, hi ha ***phishing*** **telefònic,** de vegades anomenats *phishing* de veu o "*vishing*,". En aquest cas el *phisher* truca afirmant representar el seu banc local, la policia o fins i tot l'Agència Tributària. A continuació, us espanten amb algun tipus de problema i insisteixen que ho solucioneu immediatament facilitant la vostra informació de compte o pagant una multa. Normalment us demanen que pagueu amb una transferència bancària o amb targetes prepagament, perquè són impossibles de rastrejar. El *phishing* telefònic també té la seva variant via SMS, el ***smishing***, que realitza el mateix tipus d'estafa (algunes vegades amb un enllaç maliciós incorporat on fer clic) per mitjà d'un missatge de text SMS.

[ÍNDICE]

3 S'HA D'ESTAR ALERTA. COM DETECTAR /RECONÈIXER UN MISSATGE DE *PHISHING*?

Com dèiem la majoria utilitzen la manipulació en el disseny del correu electrònic per aconseguir fer-se passar per un tercer que és conegut o de la nostra confiança. Algunes vegades els missatges no són gaire bons, salta a vista que són un frau, però d'altres estan tan ben fets que no és senzill reconèixer-los.

A continuació us donarem alguns **consells que us poden ajudar a identificar-los** juntament amb una mica de disciplina i una mica de sentit comú. Cal cercar els detalls rars o inusuals i pensar abans d'actuar. Molts missatges de *phishing* busquen ficar-nos por (per exemple: el teu compte de correu serà eliminat, el teu compte bancari bloquejat...) perquè reaccionem ràpid i sense pensar.



[ÍNDICE]

Senyals que podem cercar:

- **El contingut és sospitós?**

El primer pas per identificar un *phishing* és valorar el contingut del missatge o correu electrònic. L'intent de suplantació pot ser un banc, una plataforma de pagament, una xarxa social, un servei públic, etc.

L'objectiu és intentar espantar l'usuari i instar-lo a actuar segons les indicacions del missatge. Sempre afegeixen una excusa, exemple “problemes tècnics o de seguretat”, i proporcionen una solució senzilla del tipus “accediu al vostre banc utilitzant aquest enllaç”. A més, és molt habitual que sol·licitin nom d'usuari, claus i altres dades d'accés als comptes, **pràctica que les entitats legítimes mai no durien a terme.**

Per exemple, si no som clients d'un banc que ens escriu per dir-nos que ens bloquejarà el nostre compte si no fem certa operativa per solucionar-ho, hem de sospitar i no caure al parany. I si per casualitat som clients d'aquest banc, el millor és que anem directament pel nostre compte a la web del banc i vegem si realment passa alguna cosa amb el nostre compte o, si tenim dubtes, podem contactar per una altra via (telèfon, en persona ...) amb el nostre banc i aclarir-lo, **però mai fer clic als enllaços que ens ofereix aquest correu electrònic.**

O si el correu electrònic fa una oferta que sembla massa bona per ser veritat. Podria dir que ha guanyat la loteria, un premi car, o alguna altra cosa de valor molt elevat, ja que d'entrada és per sospitar. I l'equació: sol·licitud de dades bancàries + dades personals = frau, no sol fallar.

[ÍNDICE]

- **L'escriptura és correcta?**

Sovint en aquests missatges podem veure que no s'han utilitzat titlles, que hi ha errors gramaticals com ene en lloc d'enye, errors de puntuació... És estrany que una entitat enviï una comunicació als seus clients amb una redacció i ortografia descurades, això ens ha de fer sospitar.

Moltes vegades aquestes campanyes d'estafa les fan estrangers que tradueixen els missatges a l'espanyol amb traductors que generen errors, com ara:

- Falles semàntiques: articles “el” o “la” intercanviats.
- Paraules amb símbols estranys: on haurien d'haver-hi paraules accentuades, per exemple: “DescripciÃ³”.
- Frases mal construïdes.

Si detectem que el correu té una ortografia pobra i la seva escriptura és informal, cal estar alerta.

Sabem com ens escriuen i quins tipus de missatges ens envien les entitats amb què ens relacionem. Per exemple, des de Pangea us enviem missatges informatius i avisos sempre en català i castellà i mai us demanem les vostres dades, ja que les que necessitem ja ens les heu facilitat en fer-vos socis/es, així que si rebeu un missatge nostre en anglès o demanant segons quines dades, sospiteu!

[ÍNDICE]

- **A qui va dirigit el correu?**

Si un delinqüent vol estafar centenars de milers de persones, és molt complicat saber el nom de totes aquestes persones. Per això, utilitzen fórmules genèriques com “Apreciat client”, “Hola”, “Hola amic”, etc. per evitar dir un nom.

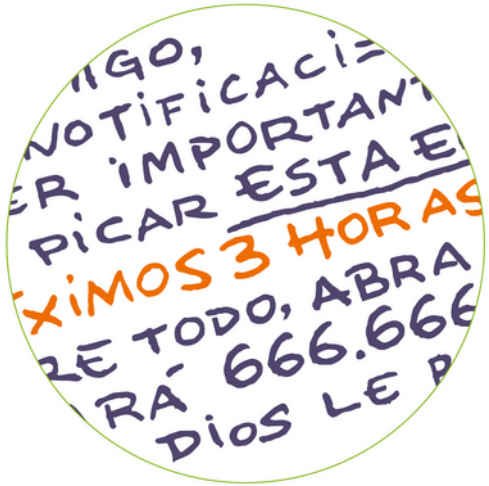
Quan una entitat ha d'adreçar-se per correu a un usuari o client, sol fer-ho enviant correus electrònics personalitzats, on utilitzarà el nom de la persona i fins i tot algunes vegades, part del seu DNI. Si rebem un correu no personalitzat, hem d'estar alerta i mirar-ho bé abans de respondre o fer el que ens demana.

- **Demana fer alguna cosa de manera urgent?**

Una altra tècnica utilitzada pels delinqüents és la de demanar la realització d'una acció en un període de temps molt curt: “Un cop emès aquest correu electrònic, tindrà un termini de 8 hores per dur a terme aquesta acció, altrament…”.

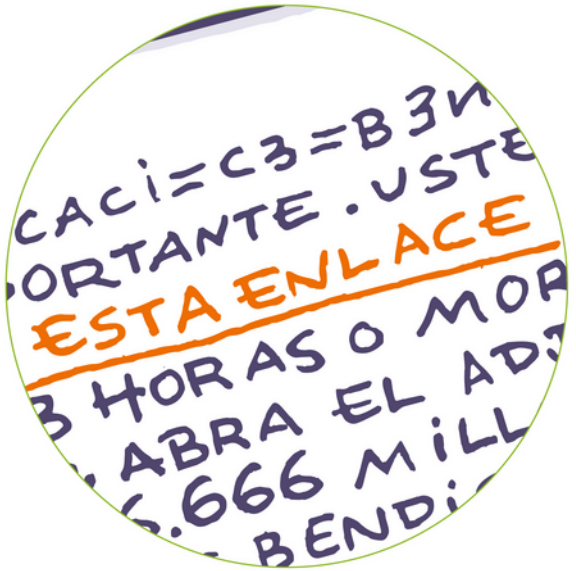
Amb aquesta urgència, els delinqüents intenten que la seva víctima prengui una decisió precipitada i caigui al parany, que inclou visitar un enllaç i indicar dades personals i/o contrasenyes.

Si el missatge sona aterridor, té un llenguatge alarmista per crear un sentit d'urgència, instant a fer clic i “actuar ràpid” abans que s'elimini el compte, o es bloquegi... és un altre símptoma que ens fa sospitar que el missatge rebut ha estat enviat per un delinqüent.



[ÍNDICE]

- **L'enllaç és fiable? i els adjunts?**



La intenció dels delinqüents és que fem clic en un enllaç per portar-nos a un lloc web fraudulent. Al text del missatge hi ha un enllaç que en lloc de portar-te a la web oficial, pàgina legítima, et porta a una altra fraudulenta que estèticament és igual o molt semblant.

Com podem saber la veritable adreça a què apunta un enllaç? Molt fàcil: situant el punter a sobre de l'enllaç i observant la veritable adreça que es mostra a la part inferior esquerra del navegador o del client de correu.

Una recomanació a seguir és la de no accedir a una web mitjançant un enllaç al correu electrònic. Si volem accedir al web legítim, la millor pràctica és escriure directament a la barra d'adreces del navegador l'adreça desitjada (si es coneix prèviament).

Si el missatge conté fitxers adjunts inesperats o estranys, cal anar amb compte, aquests adjunts poden contenir *malware*, *ransomware* o alguna altra amenaça en línia. És important tenir un antivirus o aplicació que ens permeti revisar abans d'obrir-los.

- **Qui envia el correu?**

Comprovar la identitat del remitent és important i complicat alhora, ja que no ofereix garanties per saber del cert si un correu és fiable o no.

Hem de sospitar si el remitent és una adreça de correu que no pertany a l'entitat a què el missatge fa referència i el correu electrònic del remitent no fa cap al·lusió a aquest servei. Per exemple, si rebem un correu de Pangea però l'adreça no és @pangea.org ja és per començar a sospitar.

[ÍNDICE]

Però el fet que el correu provingui d'un correu aparentment correcte no és indici concloent de la seva legitimitat. El remitent d'un correu electrònic pot estar manipulat, com expliquem a una altra de les nostres guies sobre correu. Els ciberdelinqüents són capaços d'enviar correus amb el remitent falsificat.

Si reconeixes el remitent, però és algú amb qui no tractes o que no et comuniques normalment, o encara que ho sigui, però el contingut del correu electrònic no té res a veure amb els correus habituals o són d'un tema totalment aliè a aquesta persona, o no és una cosa que esperis... el millor és sospitar.

[ÍNDICE]

4 QUÈ FER SI DETECTES UN MISSATGE DE *PHISHING*?

El bàsic és el següent:

- **No responguis** el missatge.
- **No facilitis la informació** que et demanen. Si tens dubtes pots consultar-nos o pots posar-te en contacte amb l'empresa o el servei que se suposa que representen a través dels canals oficials.
- **No accedeixis als enllaços** facilitats al missatge ni descarreguis cap document adjunt, podria tractar-se de malware.
- **Elimina-ho** i si pots, **alerta els teus contactes** sobre aquest frau perquè no caiguin tampoc al parany.

Si vols pots avisar-nos per veure si podem establir noves regles al nostre filtre antispam que puguin ajudar a detectar-lo i filtrar-lo.

[ÍNDICE]

5 QUÈ FER SI SOM VÍCTIMES D'UN *PHISHING*?

El primer si creiem estar davant d'un correu fraudulent, com hem dit, és ignorar el missatge i eliminar-lo, i per descomptat, no fer clic a cap enllaç ni descarregar cap fitxer adjunt del correu.

Si tenim la sospita d'haver estat víctima d'un d'aquests correus, cal **recopilar tota la informació** possible: correus, captures de converses mitjançant missatgeria electrònica, documentació enviada, etc.

1. Escanejar el nostre dispositiu amb un **antivirus** actualitzat.
2. **Eliminar qualsevol fitxer** que haguem descarregat del correu.
3. **Canviar les nostres contrasenyes** dels comptes implicats.
4. **Activar la verificació en dos passos** als comptes que ho permetin per evitar la suplantació d'identitat.
5. Per als casos de *phishing* bancari, **contacteu amb la vostra oficina bancària** per informar-los del que ha passat amb el teu compte online.

NOTA

És molt recomanable no fer servir la mateixa contrasenya en diferents comptes i serveis. I les contrasenyes han de complir un mínim de requisits per ser segures.

/ No utilitzar informació personal a la contrasenya (com el teu nom, data de naixement, etc.)

/ No utilitzar patrons de teclat (qwerty) ni números en seqüència (1234).

/ No utilitzeu només números, majúscules o minúscules a la contrasenya.

/ No repetiu caràcters (1111111).

/ Que tingui almenys 8 caràcters – com més caràcters, millor.

/ Que sigui una barreja de lletres majúscules i minúscules.

/ Que sigui una barreja de lletres i números.

/ Que inclogui almenys un caràcter especial, per exemple: #!@] *($

[ÍNDICE]

6. Per últim, **presentar una denúncia** davant l'autoritat pertinent.

   - En alguns casos pot ser suficient contactar amb el servei o empresa implicada per reportar el problema. Moltes empreses ofereixen seccions d'"ajuda i suport on podem denunciar el cas que ens hagi pogut afectar.

     Per exemple:

     - Una xarxa social permet denunciar un perfil fals o suplantació d'identitat.

     - Els serveis de correu electrònic compten amb mètodes de recuperació de compte en cas que hagi estat "hackejada".

     - Per eliminar comentaris d'un fòrum que atempten contra l'honor i la intimitat d'una persona, podeu contactar amb l'administrador del lloc per sol·licitar-ne la retirada.

   - A l'OSI - Oficina de seguretat de l'Internauta - de l'INCIBE (Institut Nacional de ciberseguretat) trobareu on reportar un incident de ciberseguretat: https://www.osi.es/es/reporte-de-fraude
   - Denúncia davant de les Forces de Seguretat corresponents.
     - Si ets a Catalunya t'has de dirigir a la Unitat Central de Delictes Informàtics dels Mossos d'Esquadra. (https://mossos.gencat.cat/ca/inici/)
     - Brigada de Recerca Tecnològica de la Unitat de Recerca Tecnològica (UIT) de la Policia. (https://www.policia.es/_es/denuncias.php#)

NOTA

L'OSI, canal especialitzat en ciutadans d'INCIBE, "ajuda tots els usuaris elaborant recursos de conscienciació, com els que es poden trobar a la seva campanya 'Experiència sènior', amb els quals fomenten bones pràctiques en ciberseguretat. A més, l'INCIBE posa a disposició de la ciutadania la Línia d'Ajuda en Ciberseguretat, 017, telèfon gratuït i confidencial des d'on resoldre dubtes".

6

BIBLIOGRAFÍA

- https://ca.wikipedia.org/wiki/Pesca_(inform%C3%A0tica)
- https://www.osi.es/es/banca-electronica
- https://www.osi.es/sites/default/files/docs/phishing.pdf
- https://www.osi.es/es/guia-fraudes-online
- https://www.osi.es/es/como-identificar-un-correo-electronico-malicioso

  https://es.malwarebytes.com/phishing/

[ÍNDICE]

www.pangea.org
Plaça Eusebi Güell 6-7
Edifici Vertex, planta 0
08034 Barcelona
Tel: +34 934015664
Correu: suport@pangea.org

CON EL SOPORTE DE:

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Pangea.org
< INTERNET
ÈTIC I SOLIDARI >

[ÍNDICE]