CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Com identificar el *phishing*

Document Públic

Març de 2020

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Fons Europeu de Desenvolupament Regional
Una manera de fer Europa
UNIÓ EUROPEA

CSIRT-CV és el Centre de Seguretat TIC de la Comunitat Valenciana. Naix el juny de l'any 2007 com una aposta de la Generalitat Valenciana per la seguretat en la xarxa. Va ser una iniciativa pionera en ser el primer centre d'aquestes característiques que es va crear a Espanya per a un àmbit autonòmic.

Índex de continguts

1 Què és?

La pesca (*phishing*) és el nom d'una estafa en què, a través de mitjans telemàtics, un atacant es fa passar per una empresa o organisme per a robar les dades dels seus usuaris.

El procés d'un atac de pesca és el següent: l'estafador envia un missatge, generalment a milions d'usuaris, a través d'algun mètode de comunicació (SMS, correu electrònic, fax, telèfon...) fent-se passar per alguna coneguda empresa o organització i demanant dades personals o contrasenyes als usuaris. Un percentatge d'aquests usuaris creu que el missatge és autèntic i respon amb la informació que s'hi sol·licita.

En altres ocasions els atacants falsifiquen pàgines web on copien l'aspecte de pàgines originals amb la finalitat que l'usuari es crega que són autèntiques i introduïsca les seues dades personals, contrasenyes, dades bancàries, etc.

En els dos casos, **les conseqüències** de facilitar aquestes dades poden ser el robatori de diners del compte bancari, l'ús indegut de la targeta de crèdit, l'ús de les dades per a realitzar una suplantació d'identitat, o fins i tot la venda de les dades personals.

2 *Phishing* vs. SPAM

Confondre la pesca (*phishing*) i el contingut brossa (SPAM) és un fet bastant habitual, per la qual cosa intentarem aclarir la diferència entre els dos termes.

El **contingut brossa**, o **correu no desitjat**, són correus electrònics no desitjats, generalment amb finalitats **publicitàries**. Els que produeixen contingut brossa envien els seus missatges a milers, fins i tot milions d'adreces de correu electrònic alhora esperant que el missatge arribe com més persones millor per a difondre una marca, una informació, o qualsevol classe de publicitat. El correu electrònic no és l'únic mitjà pel qual es poden rebre missatges de contingut brossa, però sí la forma més estesa.

La **pesca**, com ja s'ha comentat, és un intent d'engany a usuaris **per a robar informació personal**, contrasenyes o dades bancàries.

Per tant, cal no confondre el contingut brossa, que és publicitat no desitjada, però només publicitat al cap i a la fi, amb la pesca, l'objectiu de la qual és el robatori de dades.

3 Com podem identificar el *phishing*?

No hi ha una condició que s'haja de complir sí o sí per a saber que ens trobem davant d'un cas de *phishing*, sinó que hem de tindre alguns aspectes en consideració per a poder determinar que es tracta d'aquesta mena d'atac.

- En moltes ocasions els missatges de *phishing* no estan dirigits de manera personal. Normalment aquests fan referència a un usuari genèric com a "client", "usuari", o termes similars. També en bastants casos apareixen ocults els destinataris del missatge.

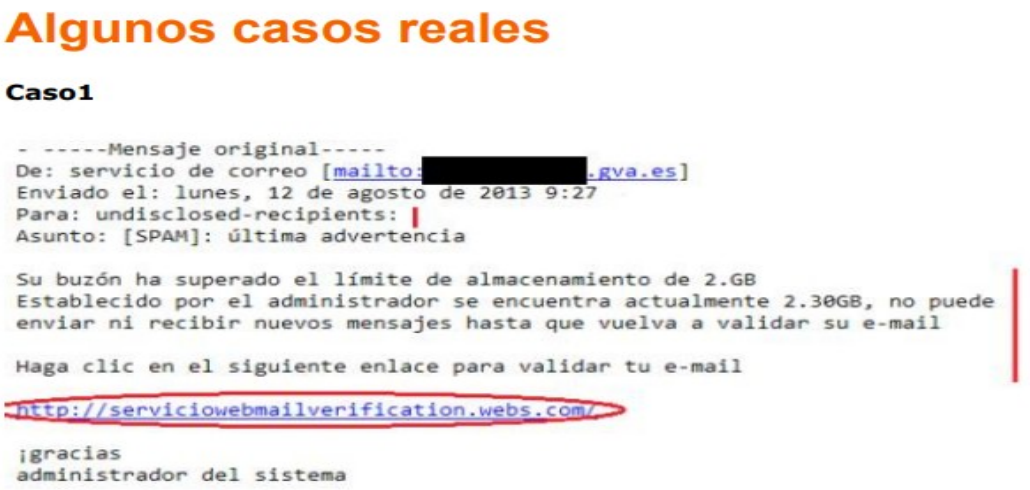
- Molts atacs de *phishing* solen contindre errors greus d'ortografia i de redacció pel fet de ser traduïts amb eines automàtiques.

- L'objectiu del *phishing* és obtindre informació, per això en els missatges o pàgines suplantades se sol·licita a l'usuari les seues dades d'accés a comptes, números de comptes bancaris o targetes de crèdit, entre altres dades.

- Alguns correus de *phishing* contenen enllaços a pàgines web on es demanen les dades als usuaris. Aquestes webs falses són fàcils d'identificar, ja que l'adreça no és la de la web autèntica: per exemple, si estan suplantant la Generalitat Valenciana, l'adreça de la pàgina web que hauria de començar amb www.gva.es/ seguit de qualsevol altra cosa. www.gva.phishing.com o www.phishing.com/gva.es, són alguns exemples de possibles adreces falses.

En trobar alguna d'aquestes evidències hem de sospitar que es tracte d'un cas de *phishing*.

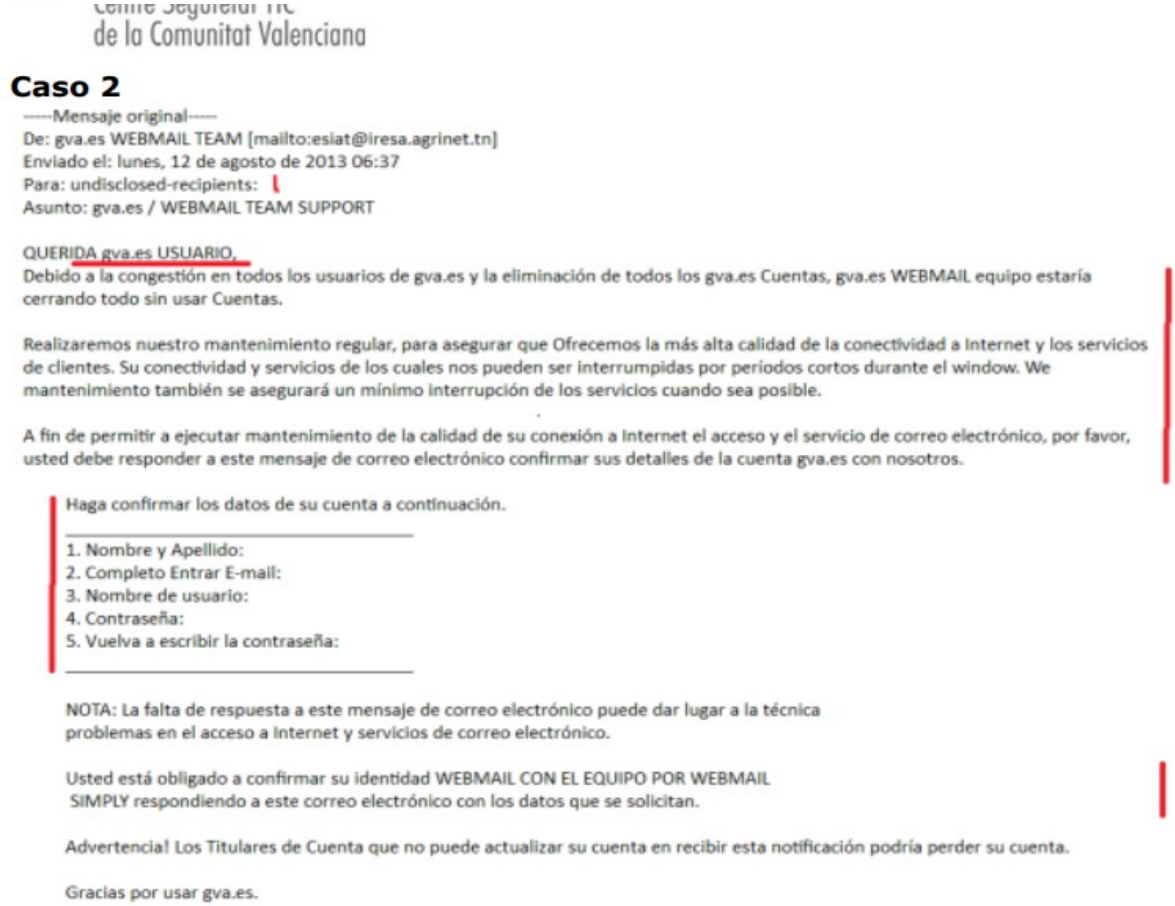
4 Alguns casos reals



En aquest cas real veiem com es compleixen totes les circumstàncies que hem comentat anteriorment per a saber que es tracta de *phishing*:

- No es dirigeix a l'usuari pel nom i desconeixem els destinataris del missatge.
- La redacció i el llenguatge que s'hi utilitza no són correctes.
- En punxar en l'enllaç apareix una web que ens demana dades personals.
- L'enllaç en el qual ens hem de validar no pertany al domini GVA.

En casos com aquest, en què les sospites que es tracte d'un cas de *phishing* són nombroses, recomanem no fer clic en l'enllaç i prendre les mesures que expliquem al final d'aquesta guia.



de la Comunitat Valenciana

Caso 2

-----Mensaje original-----
De: gva.es WEBMAIL TEAM [mailto:esiat@iresa.agrinet.tn]
Enviado el: lunes, 12 de agosto de 2013 06:37
Para: undisclosed-recipients:
Asunto: gva.es / WEBMAIL TEAM SUPPORT

QUERIDA gva.es USUARIO,
Debido a la congestión en todos los usuarios de gva.es y la eliminación de todos los gva.es Cuentas, gva.es WEBMAIL equipo estaría cerrando todo sin usar Cuentas.

Realizaremos nuestro mantenimiento regular, para asegurar que Ofrecemos la más alta calidad de la conectividad a Internet y los servicios de clientes. Su conectividad y servicios de los cuales nos pueden ser interrumpidas por períodos cortos durante el window. We mantenimiento también se asegurará un mínimo interrupción de los servicios cuando sea posible.

A fin de permitir a ejecutar mantenimiento de la calidad de su conexión a Internet el acceso y el servicio de correo electrónico, por favor, usted debe responder a este mensaje de correo electrónico confirmar sus detalles de la cuenta gva.es con nosotros.

Haga confirmar los datos de su cuenta a continuación.

1. Nombre y Apellido:
2. Completo Entrar E-mail:
3. Nombre de usuario:
4. Contraseña:
5. Vuelva a escribir la contraseña:

NOTA: La falta de respuesta a este mensaje de correo electrónico puede dar lugar a la técnica problemas en el acceso a Internet y servicios de correo electrónico.

Usted está obligado a confirmar su identidad WEBMAIL CON EL EQUIPO POR WEBMAIL SIMPLY respondiendo a este correo electrónico con los datos que se solicitan.

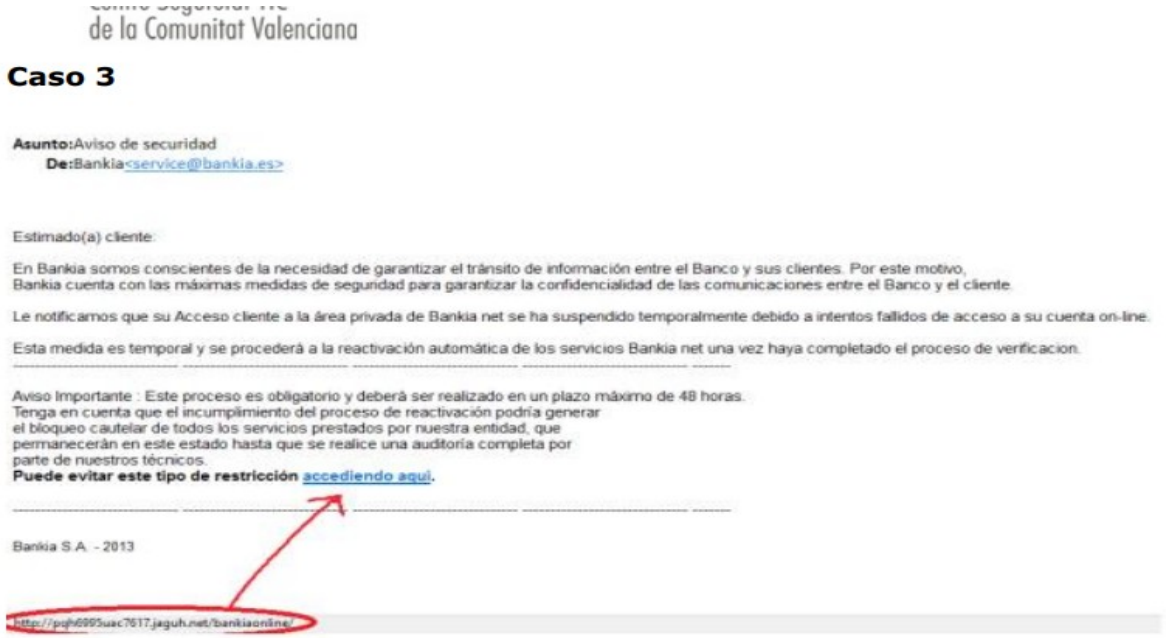
Advertencia! Los Titulares de Cuenta que no puede actualizar su cuenta en recibir esta notificación podría perder su cuenta.

Gracias por usar gva.es.

En aquest cas, també veiem que es compleixen la major part dels aspectes que ens fan saber que aquest correu es tracta d'un cas de *phishing*:

- El missatge està dirigit a un usuari genèric "Volguda gva.es USUARI".
- El llenguatge i la redacció no són correctes.
- Ens demanen dades del nostre compte entre les quals s'inclou la contrasenya.
- En aquest cas no hi ha enllaç, però l'adreça a la qual hem de respondre no és un compte @gva.es.

Després de totes aquestes evidències podem afirmar que es tracta d'un cas de *phishing*.



de la Comunitat Valenciana

Caso 3

Asunto: Aviso de securidad
De: Bankia<service@bankia.es>

Estimado(a) cliente:

En Bankia somos conscientes de la necesidad de garantizar el tránsito de información entre el Banco y sus clientes. Por este motivo, Bankia cuenta con las máximas medidas de seguridad para garantizar la confidencialidad de las comunicaciones entre el Banco y el cliente.

Le notificamos que su Acceso cliente a la área privada de Bankia net se ha suspendido temporalmente debido a intentos fallidos de acceso a su cuenta on-line.

Esta medida es temporal y se procederá a la reactivación automática de los servicios Bankia net una vez haya completado el proceso de verificacion.

Aviso Importante : Este proceso es obligatorio y deberá ser realizado en un plazo máximo de 48 horas. Tenga en cuenta que el incumplimiento del proceso de reactivación podría generar el bloqueo cautelar de todos los servicios prestados por nuestra entidad, que permanecerán en este estado hasta que se realice una auditoría completa por parte de nuestros técnicos.
Puede evitar este tipo de restricción accediendo aquí.

Bankia S.A. - 2013

http://pqh6995uac7617.jaguh.net/bankiaonline/

Una vegada més, veiem que es compleixen la major part dels aspectes que ens fan saber que aquest correu es tracta d'un cas de *phishing*:

- Es dirigeixen al destinatari com a "Estimat(a) client" sense incloure-hi el nom.
- L'ortografia és incorrecta, ja que s'utilitzen paraules com "securidad" i, en general, la redacció no és correcta.
- Si fem clic en l'enllaç ens porta a una web on ens demanen dades personals i la contrasenya d'accés.
- Si ens posem sobre el text de l'enllaç, veiem que ens porta a la pàgina http://pqh6995uac.jaguh.net/bankiaonline que res té a veure amb bankia.es.

Per tant, tot sembla indicar que es tracta d'un missatge de *phishing*.

En aquest cas, anirem un pas més enllà i veurem com podem identificar una web falsa a la qual generalment arribaríem des d'un correu de *phishing*.

Després d'accedir a la pàgina, veiem que l'aparença de la pàgina sembla legítima però abans d'introduir les dades ens fixem en la direcció del portal:

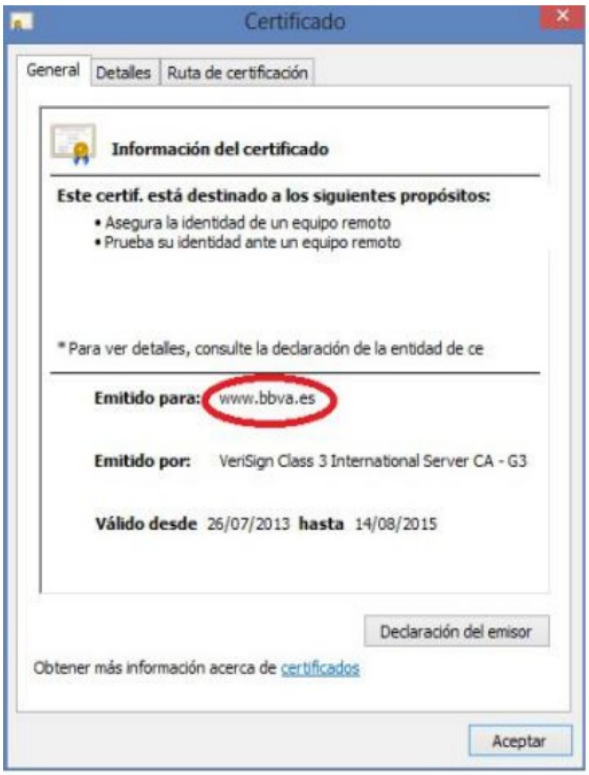
En aquest cas veiem que l'adreça és http://117.102.76.34/particulars, la qual cosa ens fa sospitar de l'autenticitat de la pàgina. L'URL real del banc en qüestió és https://www.bbva.es/, tal com veiem en la captura següent:

Com s'ha pogut comprovar, l'aparença de la web pot arribar a ser molt similar però hem d'estar atents a l'adreça de la web.

5 Seguretat en les pàgines web

Ja hem aprés a identificar correus falsos i pàgines web falses, però hi ha casos complicats en què es podria arribar a falsificar-se fins i tot l'adreça de la web. Per a evitar aquestes situacions existeixen els certificats web, que aprendrem com funcionen.

Les pàgines que necessiten nivells importants de seguretat (banca electrònica, inici de sessió, canvis de contrasenyes, etc.), tenen un certificat digital que confirma que aquesta web que s'està veient es correspon amb l'adreça que es veu en el navegador. Generalment, un cadenat verd com aquest https:// al costat de l'adreça de la web voldrà dir que la web és autèntica. Si fem clic sobre el certificat, en podrem veure els detalls:



En canvi si la web té un certificat fals, veurem que el cadenat canvia de color i a vegades es mostra una pantalla com la següent:

6 Com hem d'actuar?

En cas que es tinguen dubtes de si un correu és autèntic o si és *phishing*, el més senzill és contactar amb el remitent i preguntar-li directament si ens ha enviat el correu.

Per si mateix, el fet de rebre un correu de *phishing* no és greu i una vegada detectats es poden esborrar sense més problema, encara que és recomanable que abans d'això es remeten al **CSIRT-CV** perquè s'analitzen i s'eviten nous correus d'aquest tipus. Per a això CSIRT-CV disposa del formulari següent: https://www.csirtcv.gva.es/informar-dun-phishing/?lang=va

En cas d'haver sigut víctima d'algun atac de *phishing*, el primer que cal fer és **canviar les contrasenyes** enviades, tant per correu com formulari web. A més, si aquest fet ha causat danys, robatori de diners o d'algun tipus d'informació sensible, s'ha de **notificar a la policia** a través de la Brigada d'Investigació Tecnològica del Cos Nacional de Policia (http://www.policia.es/formulario_generico.php?ordenes=52) o el Grup de Delictes Telemàtics de la Guàrdia Civil (https://www.gdt.guardiacivil.es/webgdt/pinformar.php).

En cas de dubte, CSIRT-CV està a la vostra disposició per a garantir la seguretat TIC de la Generalitat.