Cómo identificar phishing

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

GENERALITAT VALENCIANA
CONSELLERIA DE HACIENDA Y MODELO ECONÓMICO

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Sobre CSIRT-CV

CSIRT-CV es el centro de seguridad TIC de la Generalitat Valenciana, el cual está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Conselleria de Hacienda y Modelo Económico. Este centro ofrece servicios de seguridad principalmente a la Administración Pública de la Comunidad Valenciana.

El trabajo plasmado en el presente documento ha sido sometido a un riguroso proceso de calidad que abarca desde la selección de recursos humanos hasta aspectos de auditoría y control. Confiamos en que cumpla con sus expectativas y, en caso de querer indicar algún aspecto relativo a la calidad de los servicios de CSIRT-CV, le rogamos se ponga en contacto con nosotros.

Datos de contacto

Centro de Seguridad TIC de la Comunitat Valenciana
http://www.csirtcv.gva.es/
Generalitat de la Comunitat Valenciana,
Teléfono: +34-96-398-5300
csirtcv@gva.es
https://www.facebook.com/csirtcv
https://twitter.com/csirtcv

Índice de contenido

¿QUÉ ES? **3**

PHISHING VS SPAM **4**

¿CÓMO IDENTIFICAR EL PHISHING? **5**

ALGUNOS CASOS REALES **6**

SEGURIDAD EN LAS PÁGINAS WEB **10**

¿CÓMO ACTUAR? **11**

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

¿Qué es?

El phishing es el nombre de una estafa donde, a través de medios telemáticos, un atacante se hace pasar por una empresa u organismo para robar los datos de sus usuarios.

El proceso de un ataque de phishing es el siguiente: el estafador envía un mensaje, generalmente a millones de usuarios, a través de algún método de comunicación (SMS, correo electrónico, fax, teléfono,..) haciéndose pasar por alguna conocida empresa u organización y pidiendo datos personales o contraseñas a los usuarios. Un porcentaje de estos usuarios cree que el mensaje es auténtico y responde con la información que en él se solicita.

En otras ocasiones los atacantes falsifican páginas web donde copian el aspecto de páginas originales con el fin de que el usuario se crea que son auténticas e introduzca sus datos personales, contraseñas, datos bancarios, etc.

En ambos casos, **las consecuencias** de facilitar estos datos pueden ser el robo de dinero de la cuenta bancaria, el uso indebido de la tarjeta de crédito, el uso de los datos para realizar una suplantación de identidad, o incluso la venta de los datos personales.

Phishing vs Spam

Confundir el *phishing* y el *spam* es algo bastante habitual, por lo que vamos a intentar aclarar la diferencia entre ambos términos.

El ***spam*, o correo basura,** son correos electrónicos no deseados, generalmente con fines **publicitarios**. Los *spammers* envían sus mensajes a miles, incluso millones de direcciones de correo electrónico a la vez esperando que el mensaje llegue a cuantas más personas mejor para difundir una marca, una información, o cualquier tipo de publicidad. El correo electrónico no es el único medio por el cual se pueden recibir mensajes de *spam*, pero sí la forma más extendida.

El ***phishing***, como ya se ha comentado, es un intento de engaño a usuarios **para robar información personal**, contraseñas o datos bancarios.

Por tanto no hay que confundir el *spam*, que es publicidad no deseada, pero solo publicidad al fin y al cabo, con el *phishing*, cuyo objetivo es el robo de datos.

¿Cómo identificar el phishing?

No hay una condición que se tenga que cumplir sí o sí para saber que estamos ante un caso de *phishing*, sino que debemos tener algunos aspectos en consideración para poder determinar que se trata de este tipo de ataque.

- En muchas ocasiones los mensajes de *phishing* no están dirigidos de manera personal. Normalmente éstos hacen referencia a un usuario genérico como "cliente", "usuario", o términos similares. También en bastantes casos aparecen ocultos los destinatarios del mensaje.

- Muchos ataques de *phishing* suelen contener errores graves de ortografía y de redacción por ser traducidos con herramientas automáticas.

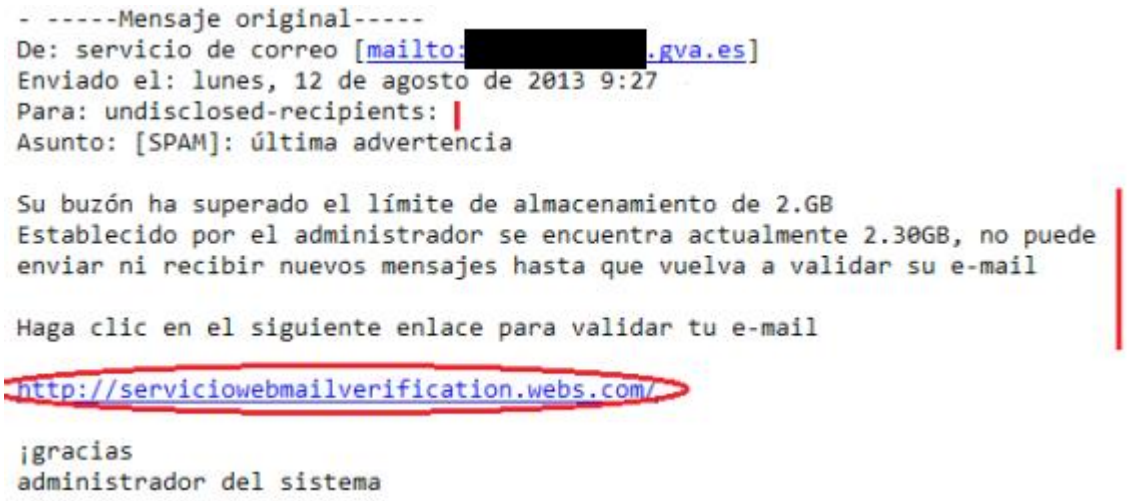
- El objetivo del *phishing* es obtener información por lo que en los mensajes o páginas suplantadas se solicita al usuario sus datos de acceso a cuentas, números de cuentas bancarias o tarjetas de crédito, entre otros datos.

- Algunos correos de *phishing* contienen enlaces a páginas web donde se piden los datos a los usuarios. Estas webs falsas son fáciles de identificar ya que la dirección no es la de la web auténtica: por ejemplo, si están suplantando a la Generalitat Valenciana, la dirección de la página web que debería de comenzar con www.gva.es/ seguido de cualquier otra cosa. www.gva.phishing.com o www.phisging.com/gva.es, son algunos ejemplos de posibles direcciones falsas.

Al encontrar alguna de estas evidencias debemos sospechar que se trate de un caso de *phishing*.

Algunos casos reales

Caso1



- -----Mensaje original-----
De: servicio de correo [mailto:[redacted].gva.es]
Enviado el: lunes, 12 de agosto de 2013 9:27
Para: undisclosed-recipients:
Asunto: [SPAM]: última advertencia

Su buzón ha superado el límite de almacenamiento de 2.GB
Establecido por el administrador se encuentra actualmente 2.30GB, no puede enviar ni recibir nuevos mensajes hasta que vuelva a validar su e-mail

Haga clic en el siguiente enlace para validar tu e-mail

http://serviciowebmailverification.webs.com/

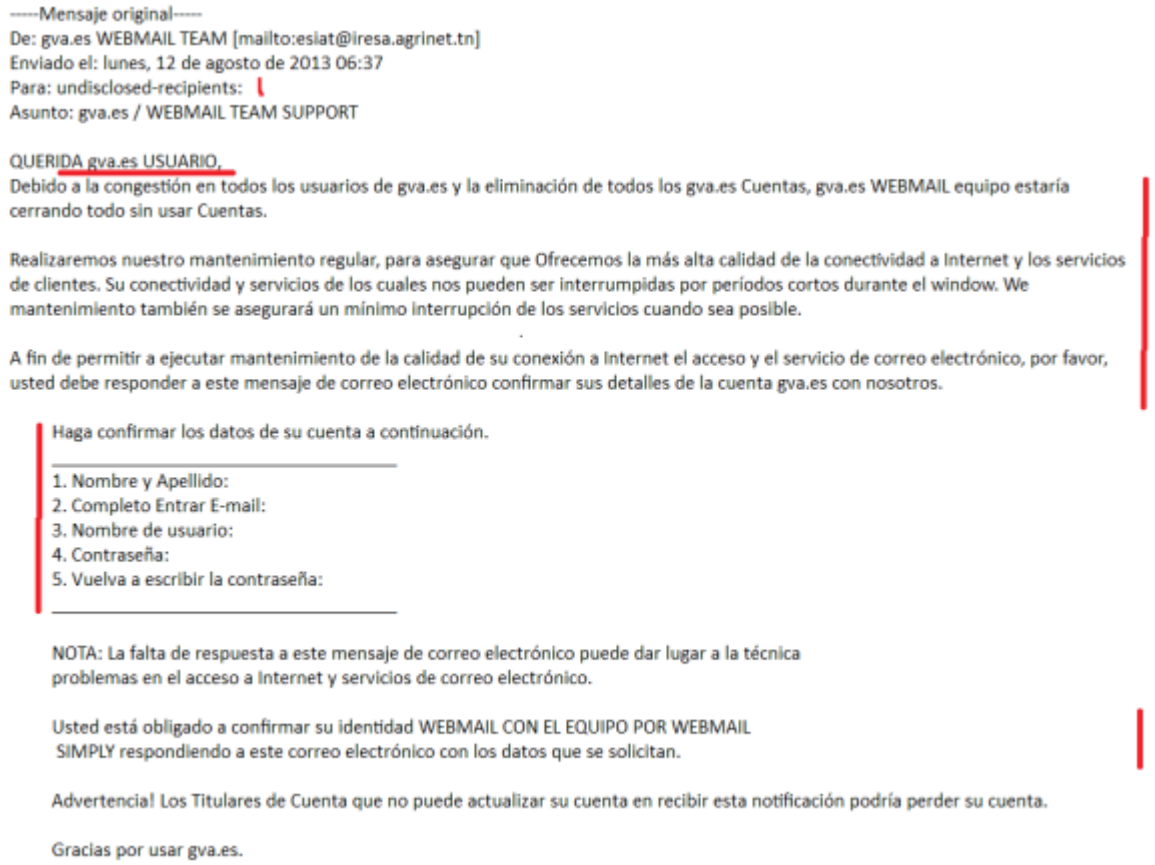
¡gracias
administrador del sistema

En este caso real vemos como se cumplen todas las circunstancias que hemos comentado anteriormente para saber que se trata de *phishing*:

- No se dirige al usuario por su nombre y desconocemos los destinatarios del mensaje.
- La redacción y el lenguaje utilizado en el mismo no son correctos.
- Al pinchar en el enlace aparece una web que nos pide datos personales.
- El enlace en el que nos debemos validar no pertenece al dominio GVA.

En casos como este donde las sospechas de que se trate de un caso de *phishing* son numerosas recomendamos no pinchar en el enlace y tomar las medidas que explicamos al final de esta guía.

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 este caso también vemos que se cumplen la mayoría de los aspectos que nos hacen saber que este correo se trata de un caso de *phishing*:

- El mensaje está dirigido a un usuario genérico "Querida gva.es USUARIO".
- El lenguaje y la redacción no son correctos.
- Se nos solicitan datos de nuestra cuenta entre los que se incluye la contraseña.
- En este caso no hay enlace, pero la dirección a la que debemos responder no es una cuenta @gva.es.

Después de todas estas evidencias podemos afirmar que se trata de un caso de *phishing*.

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 vez más, vemos que se cumplen la mayoría de los aspectos que nos hacen saber que este correo se trata de un caso de *phishing*:

- Se dirigen al destinatario como "Estimado(a) cliente" sin incluir el nombre.
- La ortografía es incorrecta, ya que se utilizan palabras como "securidad", y en general redacción no es correcta.
- Si hacemos clic en el enlace nos lleva a una web donde nos piden datos personales y la contraseña de acceso.
- Si nos ponemos sobre el texto del enlace vemos que nos lleva a la página http://pqh6995uac.jaguh.net/bankiaonline que nada tiene que ver con bankia.es.

Por tanto todo parece indicar que se trata de un mensaje de *phishing*.

Caso 4 [extraído de hijosdigitales.es]

En este caso vamos a ir un paso más allá y veremos cómo identificar una web falsa a la que generalmente llegaríamos desde un correo de *phishing*.

Tras acceder a la página vemos que la apariencia de la página aparentemente es legítima pero antes de introducir los datos nos fijamos en la dirección del portal:

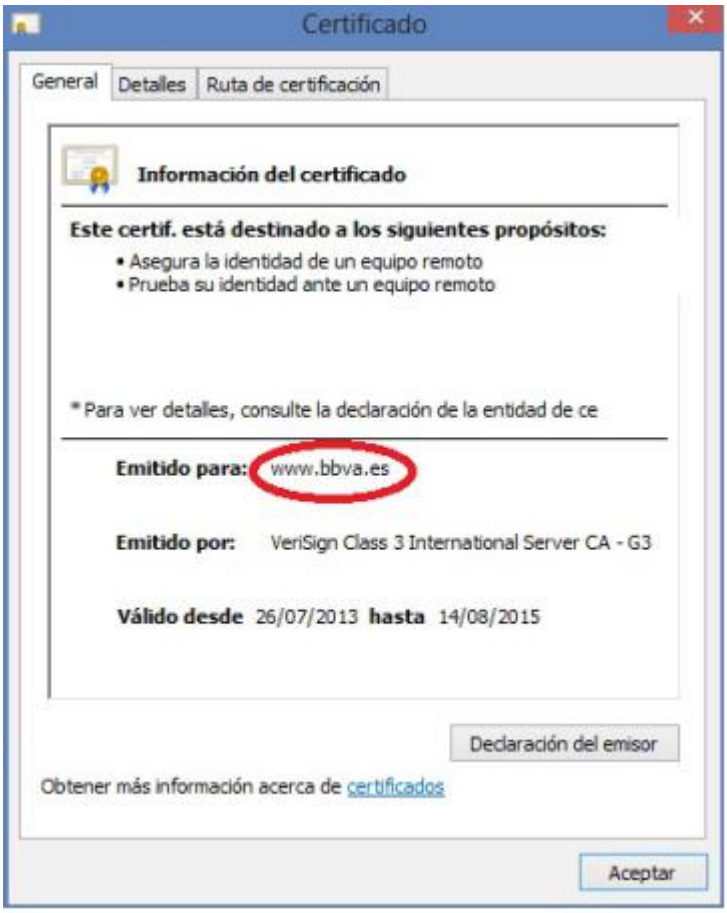
En este caso vemos que la dirección es http://117.102.76.34/particulares, lo que nos hace sospechar de la autenticidad de la página. La URL real del banco en cuestión es https://www.bbva.es/ tal y como vemos en la siguiente captura:

Como se ha podido comprobar la apariencia de la web puede llegar a ser muy similar pero hemos de estar atentos a la dirección de la web.

Seguridad en las páginas web

Ya hemos aprendido a identificar correos falsos y páginas web falsas, pero existen casos complicados en los que se podría llegar a falsificarse incluso la dirección de la web. Para evitar estas situaciones existen los certificados web, los cuales vamos a aprender cómo funcionan.

Las páginas que necesitan niveles importantes de seguridad (banca electrónica, inicio de sesión, cambios de contraseñas, etc.), tienen un certificado digital que confirma que esa web que se está viendo se corresponde con la dirección que se ve en el navegador. Generalmente un candado verde como este https:// junto a la dirección de la web querrá decir que la web es auténtica. Si hacemos clic sobre el certificado podremos ver sus detalles:



En cambio si la web tiene un certificado falso veremos que el candado cambia de color  y en ocasiones se muestra una pantalla como la siguiente:

¿Cómo actuar?

En caso de que se tengan dudas de si un correo es auténtico o si es *phishing* lo más sencillo es contactar con el remitente y preguntarle directamente si nos ha enviado el correo.

Por si mismo recibir un correo de *phishing* no es grave y una vez detectados se pueden borrar sin mayor problema, aunque es recomendable que antes de eso se remitan al **CSIRT-CV** para que se analicen y se eviten nuevos correos de este tipo. Para ello CSIRT-CV dispone del siguiente formulario:

https://www.csirtcv.gva.es/es/formulario/informar-de-un-phishing.html

En caso de haber sido víctima de algún ataque de *phishing* lo primero que se debe es **cambiar las contraseñas** enviadas ya sea por correo o formulario web. Además, si este hecho ha causado daños, robo de dinero o de algún tipo de información sensible, se debe **notificar a la policía** a través de la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía (http://www.policia.es/formulario_generico.php?ordenes=52) o el Grupo de Delitos Telemáticos de la Guardia Civil (https://www.gdt.guardiacivil.es/webgdt/pinformar.php).

En caso de duda CSIRT-CV está a vuestra disposición para garantizar la seguridad TIC de la Generalitat.