20210620, Nota Informativa, avisos de seguridad.

En virtud de mis compromisos contractuales, seguidamente os traslado los últimos tres avisos de seguridad que ha hecho públicos la Oficina de Seguridad del Internauta (OSI).

De hecho, y como ya he comentado en anteriores ocasiones, sería aconsejable consultar de forma periódica el apartado de la página web donde la OSI da a conocer las alertas; para facilitaros la cuestión os paso el enlace; a saber: https://www.osi.es/es/actualidad/avisos

Primer Aviso de Seguridad (publicado por la OSI el 18 de junio de 2021).

Se ha detectado una nueva campaña de correos electrónicos fraudulentos cuyo objetivo es **engañar al remitente para que invierta en bitcoins** tras acceder al enlace que se facilita en el correo electrónico.

Recursos afectados

Cualquier usuario que haya recibido un correo electrónico, haya accedido al enlace e introducido sus datos en el formulario de registro.

Solución

Si has recibido un correo de este estilo, no contestes, no accedas al enlace y elimínalo. Se trata de un engaño que utiliza estrategias de ingeniería social.

En el caso de que hayas accedido al enlace y hayas facilitado tus datos personales y/o bancarios, es aconsejable contactar e informar a la entidad bancaria para que tome las medidas de seguridad pertinentes.

Recopila todas las evidencias de las que dispongas (capturas de pantalla, e-mails, mensajes, etc.) y contacta con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) para presentar una denuncia si es

necesario.

Además, te recomendamos permanecer atento y monitorizar periódicamente la información que hay publicada sobre ti en Internet para evitar que tus datos privados estén siendo utilizados sin tu consentimiento.

Si, tras haber hecho *egosurfing* (es decir, una búsqueda de tu nombre y otros datos personales en el buscador), encuentras algo que no te gusta o se está ofreciendo indebidamente información sobre ti, puedes ejercer tus derechos de acceso, rectificación, oposición y supresión al tratamiento de tus datos personales. La Agencia Española de Protección de Datos te proporciona las pautas para que los puedas ejercer.

Evita ser víctima de fraudes de este tipo siguiendo las siguientes recomendaciones:

1. Si te llegan correos que no esperabas o no has solicitado y más si provienen de desconocidos, no los abras y elimínalos.
2. No contestes en ningún caso a estos correos, ni facilites información personal.
3. Ten precaución al hacer clic en enlaces y descargar ficheros adjuntos de correos, aunque sean de contactos conocidos. Los ciberdelincuentes se apoyan en estrategias de ingeniería social para hacerte caer en la trampa
4. Analizar la URL de la página web a la que es redirigido al usuario. Si no hay certificado o si no corresponde con el sitio al que accedemos, no facilites ningún tipo de información personal: nombre de usuario, contraseña, datos bancarios, etc.
5. En ningún caso reenvíes el correo, de este modo ayudarás a que no se extienda el fraude.
6. Mantén todos tus dispositivos y antivirus actualizados.

7. Recuerda contrastar toda la información que recibas en fuentes oficiales.

Detalles:

El correo electrónico fraudulento se envía desde una cuenta posiblemente falsa, generada a través de la técnica *email spoofing*. Además, dentro de los destinatarios podrían aparecer en copia direcciones de contactos conocidos, información obtenida tras haber sido víctimas de otros ataques.

El correo es identificado con asuntos que comienzan por 'Espero que…' como: **'Espero que estés pasando un maravilloso día', 'Espero que te vaya bien', 'Espero de corazón que estés pasando un día fantástico', ' Espero que estés disfrutando de un día increíble' 'Espero de corazón que estés pasando un bonito día de trabajo', 'Espero que estés teniendo un bonito día', 'Espero que estés pasando un día excelente', 'Espero de corazón que estés teniendo un día increíble', 'Espero que te vaya bien', 'Espero que estés teniendo un gran día de trabajo'** o similares.

El contenido de este correo es una única frase llamativa que insta al usuario a pulsar sobre el enlace para ser redirigido a una página fraudulenta para invertir en bitcoins. Al final del correo aparece el nombre y/o apellidos del remitente junto a un emoticono.

Al pulsar sobre el enlace, se redirige al usuario a una web fraudulenta donde podrá registrarse y, supuestamente, comenzar a invertir su dinero en bitcoins.

Segundo Aviso de Seguridad (publicado por la OSI el 15 de junio de 2021).

Se ha detectado una nueva campaña de correos electrónicos fraudulentos cuyo objetivo es extorsionar a las víctimas para que paguen una determinada cantidad en bitcoins a cambio de no publicar supuestas grabaciones íntimas. Este engaño se conoce como sextorsión.

Recursos afectados

Cualquier usuario que haya recibido un correo electrónico con características similares y haya realizado el pago.

Solución

Si has recibido un correo de este estilo, no contestes y elimínalo. Nadie ha tenido acceso a tus dispositivos, ni ha grabado un vídeo íntimo, se trata de un engaño que utiliza estrategias de ingeniería social.

MUY IMPORTANTE: no pagues ninguna cantidad a los extorsionadores, ni contestes al correo electrónico que te han enviado. Esto último sirve a los ciberdelincuentes para saber si la cuenta está activa y enviar nuevos fraudes en el futuro.

En el caso de que hayas accedido al chantaje y realizado el pago de bitcoins, recopila todas las evidencias de las que dispongas (capturas de pantalla, e-mails, mensajes, etc.) y contacta con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) para presentar una denuncia.

Evita ser víctima de fraudes de este tipo siguiendo las siguientes recomendaciones:

- Si te llegan correos que no has solicitado o de desconocidos, no los abras y elimínalos.
- No contestes en ningún caso a estos correos, ni envíes información personal.

- Mantén todos tus dispositivos y antivirus actualizados.
- En ningún caso envíes datos de tus contactos, ni reenvíes el correo, de este modo ayudarás a que no se extienda el fraude.
- En caso de duda, consulta directamente con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) o la Oficina de Seguridad del Internauta (OSI).

Detalles

El correo electrónico fraudulento se envía desde una cuenta de correo generada, posiblemente, de forma aleatoria. El asunto con el que se identifica el correo es el siguiente: '**Confirmación de transferencia de dinero**', aunque no se descarta que existan otros correos con asuntos similares. El cuerpo del mensaje está escrito en castellano y aunque no presenta faltas de ortografía, la gramática y el vocabulario no son los utilizados por una persona nativa y posiblemente derive de una traducción de otro idioma. Igualmente no se descarta que puedan aparecer otros mensajes diferentes a los del ejemplo, pero con el mismo fin.

En el cuerpo del mensaje se indica a la víctima que se ha infectado su dispositivo con un *software* espía con el que han conseguido supuestos vídeos íntimos. Los ciberdelincuentes amenazas con difundir estos vídeos entre los contactos del destinatario del correo, a no ser que realice un pago en bitcoins, para que la transacción no deje rastro, en un plazo de 48 horas. El objetivo de este plazo es evitar que la víctima se pare a pensar y analizar lo que está sucediendo y realice el pago a la mayor brevedad posible.

Tercer Aviso de Seguridad (publicado por la OSI el 10 de junio de 2021).

Se han detectado varias campañas de envío de correos electrónicos (*phishing*) y SMS (*smishing*) fraudulentos que suplantan a entidades bancarias como CaixaBank, Santander y BBVA, cuyo objetivo es dirigir a la víctima a una página web falsa para robar sus credenciales de acceso a través de diferentes engaños mediante técnicas de ingeniería social.

Recursos afectados

Usuarios que hayan recibido el mensaje, accedido a la web e introducido sus datos en la página web fraudulenta.

Solución

Si has recibido un correo o mensaje de estas características, accedido al enlace y facilitado tus datos de acceso (NIF, identificador, contraseña o número de teléfono), contacta lo antes posible con la entidad bancaria para informarles de lo sucedido. Además, te recomendamos modificar la contraseña de todos aquellos servicios en los que se utilice la misma y comenzar a usar contraseñas únicas por servicio.

Evita ser víctima de fraudes de tipo *phishing* siguiendo las siguientes recomendaciones:

1. No abras correos de usuarios desconocidos o que no hayas solicitado, elimínalos directamente. No contestes en ningún caso a estos correos.
2. Ten precaución al seguir enlaces y descargar ficheros adjuntos de correos, aunque sean de contactos conocidos. Lo ciberdelincuentes se apoyan en estrategias de ingeniería social para hacerte caer en la trampa
3. Revisa la URL de la página web. Si no hay certificado, o si no

corresponde con el sitio al que accedemos, no facilites ningún tipo de información personal: nombre de usuario, contraseña, datos bancarios, etc.

Como en cualquier otro caso de *phishing*, extrema las precauciones y avisa a tus contactos para que estén alerta de los correos que reciban de origen sospechoso, especialmente, si contienen archivos adjuntos o como en este caso, enlaces externos a páginas de inicio de sesión.

1. Cierra todas las aplicaciones o programas antes de acceder a su web.
2. Escribe directamente la URL de la entidad en el navegador, en lugar de llegar a ella a través de enlaces disponibles desde páginas de terceros o en correos electrónicos.
3. Si prefieres hacer uso de la app del banco para los distintos trámites, asegúrate de que descargas la aplicación oficial.
4. No accedas al servicio de banca online desde dispositivos públicos, no confiables o que estén conectados a redes wifi públicas.

Aprende a identificar correos electrónicos maliciosos para no caer en engaños de este tipo con la siguiente infografía: 'Cómo identificar un correo electrónico malicioso'.

Detalles

Se han detectado varias campañas de correos electrónicos y SMS suplantando a diferentes entidades bancarias, en las que a través de diferentes excusas solicitan pulsar sobre un enlace que incluyen en el contenido del mensaje. Dicho enlace redirige a una página falsa que simula ser la página del banco y donde se solicitan las credenciales de acceso.

Los correos electrónicos detectados se identifican con asuntos como: '**Número de cliente: # XXXXX / Actualización'** o '**ßanco**

Santander' aunque no se descarta que existan otros correos con asuntos similares y/o que afecten a otras entidades bancarias además de las mencionadas.

Cabe destacar que el contenido de los mensajes suele tener fallos gramaticales. Además es común que intenten apremiar al usuario mediante algún tipo de alerta, para que pulse apresuradamente en el enlace y así no tenga tiempo para pensar y analizar su contenido.

Tras introducir las credenciales de acceso el usuario será redirigido a otra página donde se solicitarán más datos personales como el número de teléfono o incluso datos de la tarjeta de crédito.

Al final del proceso, normalmente, se redirige al usuario a la página legitima del banco, para que el usuario crea que ha surgido un error en la propia web y por ello no ha podido acceder a su cuenta, sin que sospeche que los ciberdelincuentes ya estarán en posesión de todos sus datos.

En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

Hecho, conforme a mi leal saber y entender, en Manilva, a 20 de junio de 2021,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2021.06.20 08:14:50 +02'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)