20210320, Nota Informativa, avisos de seguridad.

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

De hecho, 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 en cuestión; a saber: https://www.osi.es/es/actualidad/avisos

1) Adidas no está regalando zapatillas por el Día de la Mujer

Se ha identificado una cadena de mensajes que se difunde a través de WhatsApp en la que supuestamente se obtiene un regalo de unas zapatillas, entre otros. Si se sigue la cadena de requisitos, se llegará a un formulario donde se solicitan datos personales y bancarios.

Recursos afectados

Usuarios que hayan recibido el mensaje de WhatsApp, hayan accedido a la página web y facilitado sus datos personales y/o bancarios para recibir los supuestos premios que se le han ofrecido.

Solución

Si has recibido un mensaje de estas características, has accedido al enlace y facilitado tus datos personales y/o bancarios, entre otras posibles peticiones que te hayan podido hacer, como compartir la información con tus contactos de WhatsApp; permanece atento y monitoriza 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.

Además, es recomendable que avises a tus contactos de que les has enviado un mensaje cuyo contenido es falso para que hagan caso omiso del mismo y no resulten víctimas a su vez. Es importante poner freno a estos contenidos cuyo objetivo es desinformar y engañar a los usuarios.

Evita ser víctima de engaños y fraudes siguiendo nuestras recomendaciones:

1. No pulses sobre los enlaces que contienen este tipo de mensajes en cadena. Podrías descargar malware en tu dispositivo o redirigirte a sitios web maliciosos o fraudulentos.
2. No los reenvíes sin antes contrastar la información en fuentes oficiales.
3. En caso de duda, consulta directamente con la empresa implicada o con terceros de confianza.

Aprende a identificar fraudes y bulos con los contenidos que encontrarás en: https://www.osi.es/es/campanas/bulos-fake-news-fraudes

Por último, siempre puedes denunciar esta situación ante las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y si necesitas más

información, puedes llamar a la Línea de Ayuda en Ciberseguridad de INCIBE, 017, gratuita y confidencial.

2) Campaña de distribución de malware suplantando a diferentes servicios

Se ha detectado una nueva campaña de correos electrónicos suplantando la identidad de diferentes empresas, como WeTransfer o WhatsApp, cuyos mensajes contienen enlaces que descargan un troyano en el dispositivo. El mensaje que contiene los diferentes correos instan al usuario a pulsar sobre un enlace utilizando distintos argumentos.

Recursos afectados

Cualquier usuario que haya recibido un correo electrónico de estas características, haya pulsado sobre el enlace para consultar los supuestos archivos, como puede ser el histórico de mensajes y llamadas de WhatsApp, y posteriormente ejecutado el archivo que se descarga.

Solución

Si no has ejecutado el archivo descargado, posiblemente tu dispositivo no se habrá infectado. Lo único que debes hacer es eliminar el archivo que encontrarás en la carpeta de descargas. También deberás enviar a la papelera el correo que has recibido.

Si has descargado y ejecutado el archivo malicioso, es posible que tu dispositivo se haya infectado. Para proteger tu equip,o debes escanearlo con un antivirus actualizado o seguir los pasos que encontrarás en desinfección de dispositivos. Si necesitas soporte o asistencia para la eliminación del *malware*, INCIBE te ofrece su servicio de respuesta y soporte ante incidentes de seguridad.

Te recordamos que en caso de duda sobre la legitimidad de un correo, no debes pulsar sobre ningún enlace, ni descargar ningún archivo adjunto. Para comprobar la veracidad, puedes ponerte en contacto con la empresa o el servicio que supuestamente te ha enviado el correo, siempre a través de sus canales oficiales de atención al cliente.

Además, para mayor seguridad, es recomendable realizar copias de seguridad de manera periódica con toda la información que consideres importante para que, en caso de que tu equipo se vea afectado por algún incidente de seguridad, no la pierdas. También es recomendable mantener tus dispositivos actualizados y protegidos siempre con un antivirus.

3) Lidl no está ofreciendo a sus clientes un robot de cocina por los puntos de fidelización

Se ha detectado una campaña de envío de correos electrónicos que suplantan la identidad de Lidl. El objetivo es redirigir a la víctima a través de un enlace facilitado en el mensaje del correo a una página web fraudulenta (*phishing*). Dicha web solicita al usuario rellenar un formulario y así poder optar supuestamente a un robot de cocina por muy poca cantidad de dinero, pero no sin antes facilitar sus datos personales y bancarios.

<u>Recursos afectados</u>

Cualquier usuario que haya recibido el correo electrónico y haya introducido sus datos personales y/o los de su tarjeta bancaria en el formulario de la página fraudulenta.

Solución

Si has recibido un correo electrónico de estas características, has accedido al enlace y facilitado los datos de tu tarjeta de crédito, contacta lo antes posible con tu entidad bancaria para informarles de lo sucedido. 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 tipo *phishing* siguiendo nuestras recomendaciones:

- No te fíes de los correos electrónicos de usuarios desconocidos o que no hayas solicitado, elimínalos de tu bandeja de entrada.
- No contestes en ningún caso a estos correos.
- Ten siempre actualizado el sistema operativo y el antivirus de tu dispositivo. En el caso del antivirus, además se debe comprobar que esté activo.
- En caso de duda, consulta directamente con la empresa o servicio implicado o con terceras partes de confianza, como son las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y la Oficina de Seguridad del Internauta (OSI) de INCIBE.

Además, ten siempre en cuenta los siguientes consejos:

- Escribe directamente la URL del servicio en el navegador, en lugar de llegar a la web a través de enlaces disponibles desde páginas de terceros, en correos electrónicos o en mensajes de texto.
- No facilites tus datos personales (número de teléfono, nombre, apellidos, dirección o correo electrónico) o bancarios en cualquier página. Infórmate previamente y lee los textos legales de la web para descartar un posible mal uso de tus datos.
- Desconfía de promociones online que requieran facilitar información personal.
- En caso de acceder a un servicio desde su aplicación, revisa que tengas instalada la aplicación legítima y que los permisos proporcionados sean adecuados.

4) Oleada de casos de suplantación de identidad en cuentas de Instagram y Onlyfans con fraudes dirigidos hacia sus seguidores

En las últimas semanas se ha detectado un elevado número de cuentas de Instagram que han sido suplantadas, bien en la citada red social o en otras como OnlyFans. El objetivo sería contactar con los seguidores de las cuentas afectadas para, con diferentes estrategias de ingeniería social, es decir, de engaño, realizar algún tipo de fraude con perjuicio económico hacia la víctima.

Recursos afectados

En primer lugar aquellos usuarios que hayan sido víctimas de la suplantación de identidad de su cuenta en la red social. En segundo

lugar, los seguidores de las cuentas suplantadas que hayan sido contactados por la cuenta ilícita y hayan facilitado sus datos personales y/o bancarios o realizado algún tipo de pago.

Solución

Si has sido víctima de una suplantación de identidad de tu cuenta de una red social, sigue estas recomendaciones:

- **Bloquea la cuenta que te está suplantando** para dificultar que pueda identificar a tus seguidores y ponerse en contacto con ellos. Para bloquear un perfil de Instagram, debes entrar en el mismo y en los 3 puntos situados en la esquina superior derecha seleccionar la opción “Bloquear”.
- **Denuncia la cuenta que te está suplantando a la red social**, todas las redes sociales cuentan con mecanismos para realizar este tipo de denuncias. De esta forma la plataforma será consciente de lo que está sucediendo para tomar las medidas oportunas y cerrar el perfil falso.
    - Cómo denunciar cuentas en Instagram.
    - Cómo denunciar cuentas en OnlyFans.
- **Advierte a tus contactos sobre el perfil ilegítimo** para que estén alerta en caso de que les envíe una solicitud de amistad o se ponga en contacto con ellos y así evitar que se conviertan en víctimas del fraude a su vez.
- **Documenta todo lo ocurrido**, haciendo capturas de pantalla de los perfiles falsos y de los posibles mensajes que este envíe, tanto a ti como a tus contactos, y efectúa una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado, en caso de que lo consideres oportuno.

- **Si tu perfil es público, hazlo privado al menos hasta que se solucione el problema**, así evitarás que el ciberdelincuente pueda ver si estás alertando a tus seguidores de la cuenta falsa y dificultarás que conozca el listado de tus seguidores, aunque podría acceder a esta información igualmente si es uno de ellos.

Si has recibido algún mensaje de un perfil falso y has accedido al enlace y facilitado los datos de tu tarjeta de crédito o realizado algún tipo de pago, contacta lo antes posible con tu entidad bancaria para informarles de lo sucedido.

Además, ten siempre en cuenta los siguientes consejos:

- Desconfía de promociones o sorteos online que requieran facilitar información personal.
- Si algún perfil de una red social se pone en contacto contigo mediante mensaje directo sin que lo esperaras, cerciórate de que se trata del perfil legítimo y no es fraudulento.
- No facilites tus datos personales (número de teléfono, nombre, apellidos, dirección o correo electrónico) o bancarios en cualquier página. Infórmate previamente y lee los textos legales de la web para descartar un posible mal uso de tus 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 marzo de 2021,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2021.03.20 07:54:53 +01'00'

Salvador Zotano Sánchez

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