20210920, Nota Informativa, aviso y recomendación de seguridad.

En virtud de mis compromisos contractuales, seguidamente os participo del último aviso de seguridad emitido por la OSI (Oficina de Seguridad del Internauta, dependiente del INCIBE -Instituto Nacional de Ciberseguridad-) referente a una "oleada de correos fraudulentos de tipo phishing suplantando empresas reconocidas para ofrecer regalos tras realizar una encuesta" y una serie de recomendaciones referentes a la necesidad de borrar el historial de navegación en internet.

Se han detectado varias campañas de envío de correos electrónicos falsos que suplantan la identidad de diferentes empresas reconocidas, como Amazon, MediaMarkt o Apple. Captan la atención del usuario ofreciendo regalos de productos electrónicos y bonos de descuento. Para recibirlos, será necesario rellenar una encuesta en la que se solicitarán datos personales y bancarios. El objetivo es redirigir a la víctima, a través de un enlace facilitado en el correo, a una página web fraudulenta (*phishing*) que simula ser la del citado servicio.

Recursos afectados

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 tus datos personales y 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 las siguientes 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 debes 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) e INCIBE, a través de la Oficina de Seguridad del Internauta (OSI).

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.

En otro orden de cosas, y en relación de la necesidad de borrar el historial de navegación, decir que internet es una enorme autopista de información. Cuando navegamos por la Red y usamos nuestras redes, visitamos alguna página web o utilizamos algún programa que necesita conexión a Internet, como nuestro correo electrónico, dejamos tras de sí una serie de datos con información sobre todo lo que hacemos. Si bien esto es útil para navegar más rápidamente, también puede suponer un riesgo, por lo que conviene saber cómo eliminar este rastro digital que vamos dejando.

El navegador, que es la herramienta que utilizamos para acceder a Internet, va recogiendo y almacenando las cosas que vamos haciendo con él, es decir, las páginas que visitamos, los usuarios y contraseñas utilizados para acceder a los servicios online y muchas cosas más. Todo ello para que nuestra experiencia por la Red sea lo más sencilla posible. Sin embargo, estas ventajas pueden convertirse en un riesgo para nuestra privacidad. Por eso, es importante que aprendamos a revisar y eliminar toda aquella información que no queremos que se

quede almacenada en el navegador para que nadie pueda aprovecharse de ella.

Antes de profundizar en los riesgos y en cómo evitarlos, es necesario que entendamos algunos conceptos clave:

- **Navegador:** es el programa o herramienta que utilizamos para navegar por Internet. Los más conocidos son Microsoft Edge, Google Chrome, Mozilla Firefox o Safari (Apple).
- **Historial**: se trata de un registro de todas las webs que visitamos.
- **Cookies:** son pequeños archivos que se crean cuando visitamos páginas web y que contienen información sobre el navegador que utilizamos, nuestro idioma, si nos hemos registrado con un usuario y contraseña en alguna página, la hora de visita e incluso el dispositivo que hemos utilizado (móvil, portátil o tablet).
- **Caché:** son archivos temporales (se eliminan con el tiempo) que se guardan para que nuestra navegación vaya más rápida, como las imágenes o vídeos de webs que frecuentamos, para no tener que cargarlos cada vez que accedamos.

¿Cuáles son los riesgos de dejar un rastro cuando navegamos?

Toda la información que almacena el navegador forma un registro muy completo sobre nosotros: qué páginas nos gusta visitar (gustos e intereses), desde dónde accedemos a Internet (ubicación), con qué tipo de dispositivo (móvil, ordenador o tablet), sistema operativo, etc.; y como todo en lo referente a Internet, dejar demasiada información privada sin control puede tener consecuencias negativas.

Por ejemplo, nuestros gustos y hábitos a la hora de navegar por la Red son el objetivo de muchos ciberdelincuentes, ya que esta información es muy valiosa para lanzar campañas de publicidad maliciosas con las que tratar de hacernos caer en sus trampas.

Además, almacenar tanta información en el navegador, sin protección, es un riesgo para nuestra privacidad. Imaginemos que una persona pudiese, con tan solo un par de clics, acceder a todo el registro de webs visitadas. Podría hacerse una idea de quiénes somos, ¿verdad? Esto podría suceder simplemente compartiendo el mismo navegador al utilizar ordenadores públicos o compartidos con otros usuarios.

Por todo esto, y por mucho más, es conveniente que borremos el rastro que dejamos en el navegador cada poco tiempo.

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 septiembre de 2021,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Nombre de reconocimiento (DN): c=ES, serialNumber=IDCES-32028277H, givenName=SALVADOR, sn=ZOTANO SANCHEZ, cn=ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2021.09.20 08:35:53 +02'00'

Salvador Zotano Sánchez

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