20200620, Nota informativa, sobre la Oficina de Seguridad del Internauta.

En virtud de mis deberes contractuales, a continuación, le detallo las funciones que realiza la O.S.I. (Oficina de Seguridad del Internauta) exponiendo, como ejemplo, las dos últimas alertas realizadas por dicho organismo.

En la **Oficina de Seguridad del Internauta** (OSI) del **INCIBE** (Instituto Nacional de Ciberseguridad) se proporciona la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.

El objetivo de la OSI es reforzar la confianza en el ámbito digital a través de la formación en materia de ciberseguridad. En la OSI del INCIBE tienen como prioridad:

- Ayudar a los usuarios a llevar a cabo un cambio positivo de comportamiento en relación con la adopción de buenos hábitos de seguridad.
- Hacerles conscientes de su propia responsabilidad en relación con la ciberseguridad.
- Contribuir a minimizar el número y gravedad de incidencias de seguridad experimentadas por el usuario.

Una de las funciones que realiza es hacer saber las amenazas que se producen a través de su página web; a continuación se relacionan las dos últimas alertas.

Primera: Se han identificado nuevos correos que utilizan diferentes remitentes e intentan suplantar a diversas entidades. Todos ellos tienen el mismo denominador común: suministrar un enlace al usuario que descarga un malware bajo alguna excusa. Los nuevos correos electrónicos maliciosos captan la atención del usuario con asuntos como los siguientes: [xxx@] SU DNI ha sido bloqueado!, [xxx@] SEGUNDO AVISO!, Se envía un reembolso de la Seguridad Social, Denuncia Sanidadxxx, Intimacion Sanidadxxxxxx, Denuncia a su nombrexxx. No

se descarta que puedan estar utilizándose otros asuntos para engañar al usuario con el mismo objetivo, que haga clic en un enlace que descarga un fichero malicioso en el equipo de la víctima.

Entre los pretextos utilizados para que el usuario haga clic en el enlace malicioso, encontramos los siguientes:

- Se le informa de que su DNI ha sido bloqueado y que tiene 48 horas para apelar su defensa. Puede ver la copia del supuesto proceso haciendo clic sobre el enlace que facilitan para tal fin.
- Vence el pago de una factura y si no se efectúa un pago antes de una fecha indicada, supuestamente se procederá a la suspensión de los servicios ofrecidos por la entidad/empresa.
- Se le informa al usuario de que tiene derecho a recibir un reembolso económico y para solicitarlo debe acceder a un link.
- Se notifica al usuario que sus vecinos han interpuesto una denuncia por no usar las mascarilla. Para poder descargar la supuesta notificación se facilita un enlace.

Segunda: Se ha detectado una campaña de envío de correos electrónicos falsos que suplantan la identidad del Departamento de Aduanas. El objetivo es solicitar a la víctima que realice un pago a través del servicio *Paysafecard* para poder recibir un paquete.

El correo electrónico fraudulento se envía desde una cuenta de correo electrónico que no pertenece al departamento de aduanas de la Agencia Tributaria, ni al servicio de Correos. Se envía bajo el asunto "Notificación: DEPARTAMENTO ADUANERO REGIONAL", aunque no se descarta que puedan estar distribuyéndose mediante otros correos con asuntos similares.

La estafa avisa al usuario de que ha recibido un paquete y para permitir la entrega se facturarán los costes del IVA al destinatario del paquete.

Las principales características de este fraude son:

- El correo enviado se identifica como Departamento Aduanero Regional y firma como la Agencia tributaria ES. Aunque la dirección del remitente no tiene relación con este servicio.

- Para dar más credibilidad, se adjunta una imagen de un paquete al correo. Por nuestra seguridad, no debemos abrir archivos adjuntos de correos electrónicos sospechosos. Podría contener *malware*.

- El lenguaje utilizado es incorrecto, con numerosas faltas de ortografía e incoherencias gramaticales.

- El pago que se solicita es de 50 € a través de un servicio poco conocido, que facilita el anonimato ya que no se asocia a ninguna cuenta bancaria. Simplemente se realiza una recarga de dinero asociada a un código PIN y con ese código se puede pagar en diferentes establecimientos.

- La dirección de correo electrónico a la que se solicita enviar el código PIN se encuentra ofuscada, es decir que, en realidad, si pulsamos sobre la dirección y se abre nuestro gestor de correo con un nuevo mensaje, la dirección que aparece en el apartado del destinatario será otra totalmente distinta.

Al facilitar el código PIN a los ciberdelincuentes, ellos podrán utilizarlo para realizar pagos sin autorización de la persona que ha comprado el código.

En todo caso, quedo a su disposición para aclarar o ampliar la información relacionada en esta Nota Informativa.

Hecho, conforme a mi leal saber y entender, en Manilva a 20 de junio de 2020,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2020.06.20 11:33:03 +02'00'

Salvador Zotano Sánchez

(DPD Certificado Esquema AEPD-DPD v.1.4. Nº 19-ADK0101)