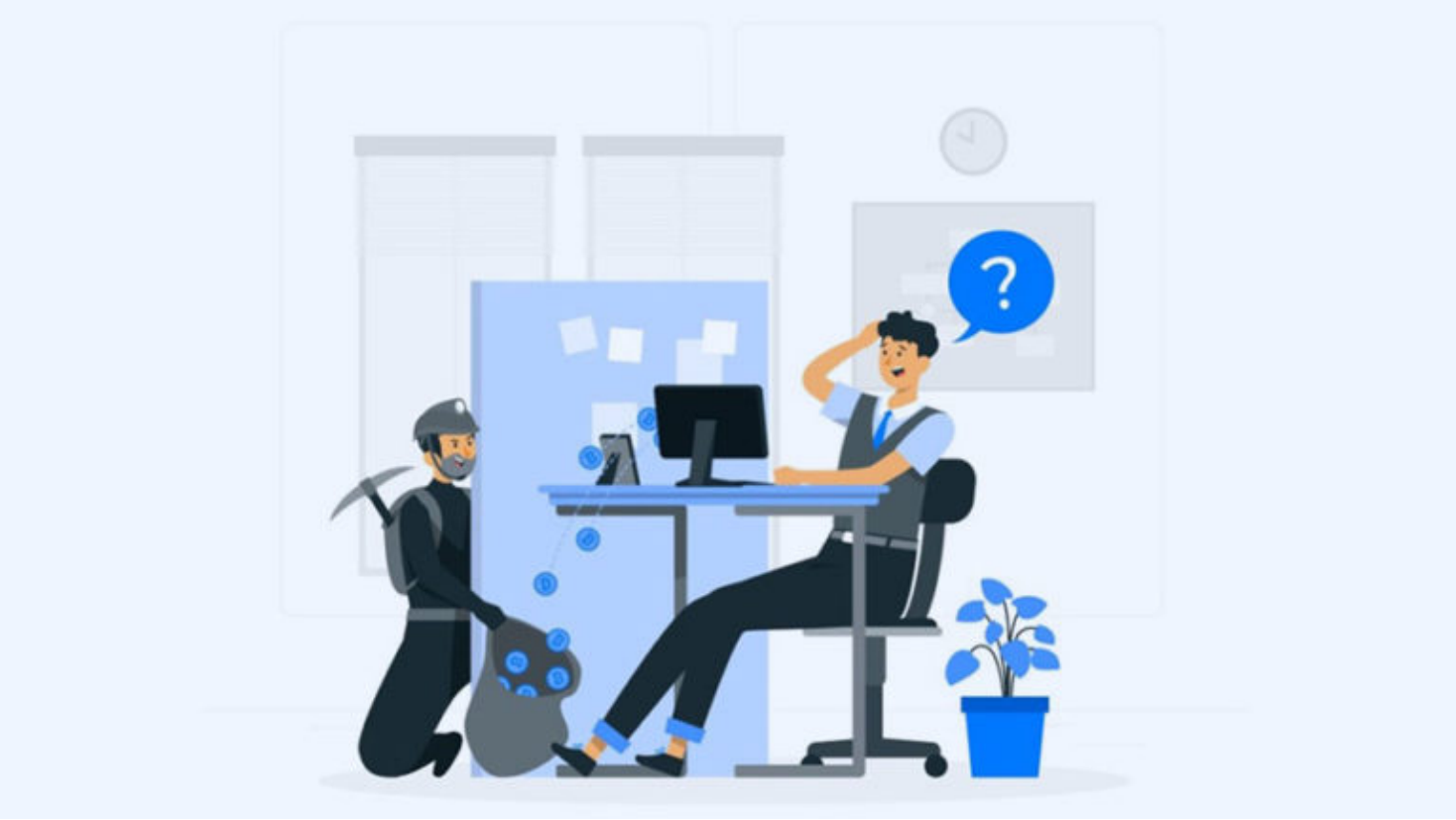
Ciberdelitos: Opciones más usuales y qué hacer para evitarlas

18 de febrero de 2022



Autor: María del Mar Molina Parra
Miembro del equipo de trabajo del Proyecto Edufinet

Los intentos de estafa por medios tecnológicos están cada vez más a “la orden del día”. No en vano en el último Congreso de Educación Financiera de Edufinet[1] se desarrolló una ponencia dedicada a estos temas impartida por el Inspector Jefe de ciberdelincuencia de la Policía Nacional en Málaga (puedes ver la ponencia íntegra aquí: https://www.youtube.com/watch?v=On-gCFwcw6w).

Y, en palabras extraídas de dicha ponencia, “El eslabón más débil en Ciberseguridad no son las máquinas, son los seres humanos”. Empieza a ser de crucial importancia que tengamos en cuenta las diferentes formas en las que los delincuentes nos pueden hacer “picar” y, por tanto, tener acceso a nuestra información financiera como paso previo para disponer ilícitamente de nuestros fondos.

En el artículo de hoy vamos a dar un pequeño repaso a los más habituales en los últimos tiempos.

1. Phishing.

En esta modalidad la posible victima recibe un correo electrónico, ya sea de una entidad financiera o una empresa de reconocido prestigio, en el que nos indican que ha habido un problema con nuestra contraseña de la banca *online*, que tenemos un paquete pendiente de recoger o incluso que nos han pagado Bitcoins.

Estos "mails" suelen incluir un enlace al que tenemos que acceder y ahí es cuando damos paso a que obtengan nuestras claves bancarias o incluso instalar un troyano en nuestro dispositivo.

Ejemplo e-mail[2] *phishing*

2. Smishing.

Esta modalidad es similar al *phishing* pero vía SMS. Recibimos en nuestro teléfono móvil un mensaje que incluye un enlace en el que tenemos que pinchar. Una vez ahí nos solicitan que introduzcamos una serie de datos personales que son utilizados a continuación, bien para acceder a nuestra información financiera o bien para utilizar nuestros datos personales en otro delito.

3. Vishing.

La opción utilizada en esta modalidad es la del teleoperador que llama por teléfono, lo que da cierta credibilidad a la posible estafa. La finalidad es la misma que en las opciones anteriores: obtención de datos.

4. Combinación de *phising, smishing y vishing.*

En esta "nueva" modalidad se combinan las tres opciones de manera que se le da mucha credibilidad a la operación. Se le envía a la "victima" un mensaje suplantando la identidad de la entidad financiera indicándole que, por ejemplo, ha de activar la seguridad o que su cuenta quedará bloqueada. El enlace en el que hay que pinchar deriva a una web que imita la de dicha entidad financiera y en la que hay que introducir los datos de acceso a la banca *online*. Una vez realizado este paso se le comunica que un empleado le llamará para realizar las últimas verificaciones de seguridad.

Esta combinación favorece la confianza de la persona que lo recibe, que no duda en realizar los pasos que se le solicitan, quedando a merced de los delincuentes.

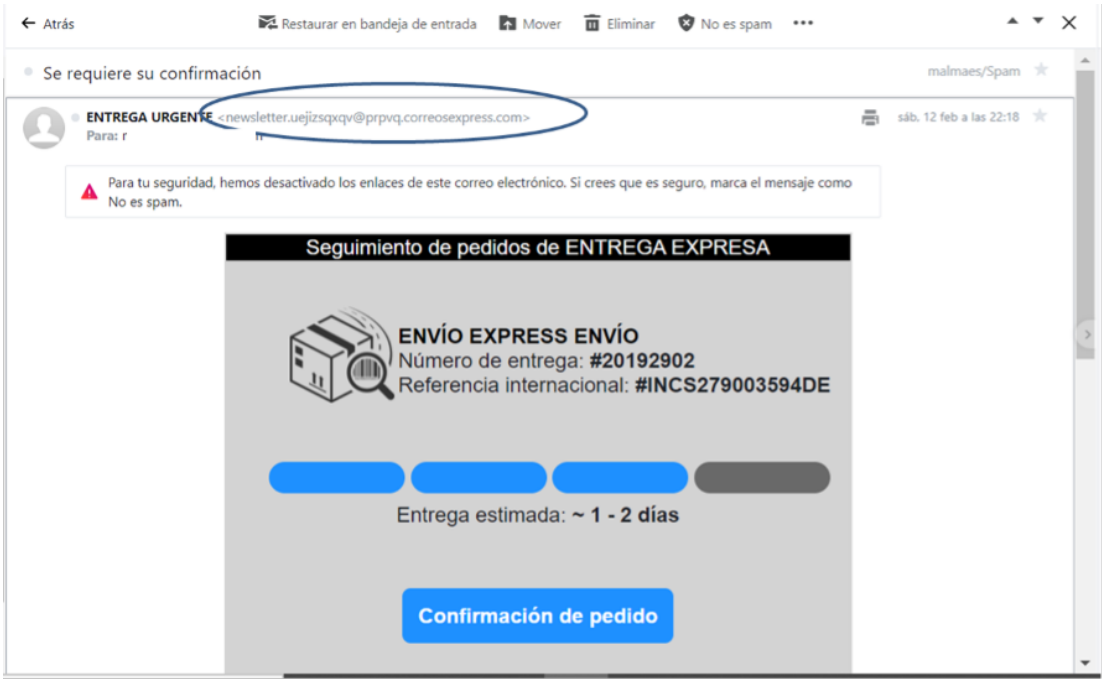
5. En otras versiones lo que se nos invita a hacer es escanear un código QR. Lo que hace que se abra un enlace que puede contener algún tipo de "software" malicioso que infecte, normalmente, nuestro teléfono móvil.

¿Cómo evitar que nos estafen por alguno de estos métodos?

Lo primero que debemos tener en cuenta es que **nuestra entidad financiera jamás nos va a solicitar que verifiquemos nuestros datos a través de un enlace enviado vía "e-mail" o mensaje de texto**. Nos pedirán que pasemos por una oficina para poder realizar todas las verificaciones y comprobaciones necesarias.

También es útil que nos fijemos en la dirección de "e-mail" desde donde nos remiten el correo, ya que este no siempre es una dirección extraña, sino que puede parecerse en gran medida a una oficial, e incluso incluir una imagen de marca real; o si el número de teléfono desde el que envían un sms o nos llaman es privado.

Ejemplos:



Ante la duda, nunca dar datos personales y recurrir siempre al origen, es decir, llamar al teléfono oficial de atención al cliente de nuestra entidad o de la empresa remitente, y confirmar la veracidad de lo que estamos recibiendo.

Pero estas no son las únicas formas que tienen los delincuentes de tratar de obtener datos o incluso hacer pagos. Las diferentes opciones de pago tampoco están exentas de este tipo de fraudes, desde los ya conocidos en los que tenemos que introducir los datos de nuestra tarjeta, que son clonados y utilizados para realizar compras *online* en webs donde no se verifica fehacientemente si el titular real de la tarjeta es el que está operando, hasta aquellos que utilizan aplicaciones de pago con teléfono móvil, por ejemplo, para recibir/enviar pagos.

En el caso de las tarjetas, en la mayoría de los pagos, ya se realiza una comprobación para validar la autenticidad del titular como es recibir un mensaje a nuestro móvil (el que hayamos indicado en nuestra entidad financiera) o que tengamos que introducir alguno de los números de los que componen el pin de nuestra tarjeta (en ningún caso los 4).

En la opción de los pagos realizados a través de dispositivos de telefonía móvil vinculados a nuestras cuentas bancarias, podemos encontramos dos modalidades:

- En el caso de que nosotros seamos los compradores, el "presunto vendedor" nos solicita el pago de una cantidad previa antes de enviarnos el bien objeto de la compra.
- En el caso de que seamos los vendedores, lo que se nos envía no es un abono sino una solicitud de cargo, es decir, en lugar de enviarnos el dinero nos solicita que se lo enviemos nosotros. Esta opción se basa en muchas ocasiones en el desconocimiento de la existencia de esta opción dentro de la aplicación.

Para evitar estas estafas tendríamos que asegurarnos de la "legalidad" del vendedor y no realizar el pago antes de tener físicamente el objeto o constancia fehaciente de su envío, o, antes de autorizar cualquier operación con el teléfono móvil, leer correctamente la notificación que se nos envía, ya que se indica que lo que estamos haciendo es autorizar un cargo en nuestra cuenta.

En resumen, el mejor consejo que se puede dar en estas situaciones es ser sumamente cuidadoso cuando no hemos solicitado una información y leer siempre a conciencia cualquier aviso que recibamos. Ante la más mínima duda, contactar de inmediato con nuestra entidad financiera.

Imagen: Vector de Seguridad creado por storyset – www.freepik.es

---

[1] IV Edición del Congreso. Se pueden ver esta y las ediciones anteriores en el canal de YouTube del Proyecto Edufinet (https://www.youtube.com/channel/UCxCStRrm_N8GMAJ9GjpD-Tw)

[2] Todas las imágenes de esta entrada están tomadas de comunicaciones ilícitas reales recibidas por su autora.