CDMX
CIUDAD DE MÉXICO
Junta de Asistencia Privada del Distrito Federal

Nueva Etapa • No.23
Martes 31 de enero de 2017.

Tecnológico

MARTES DE TIPS
EN FORTALECIMIENTO INSTITUCIONAL

Consejos para detectar
Páginas web Falsas

Comunicación | Administrativo | Legal | Asistencial | Análisis y Supervisión | Financiero | Desarrollo Institucional

Es una práctica común de la delincuencia, atraer la atención de probables víctimas con el envío de correos electrónicos que contienen supuestas alertas de cancelación o bloqueo de cuentas bancarias, o también, por el incumplimiento del pago de servicios como luz, agua o teléfono; en estos correos electrónicos solicitan información personal que posteriormente usan de manera fraudulenta.

En muchos casos, dentro del cuerpo del mensaje, piden dar clic a vínculos que redirigen a **sitios web falsos**, que emulan los sitios oficiales de bancos o de las empresas de servicios más comunes, con la intención de engañarnos y de conseguir que les entreguemos los datos personales que necesitan o, bien, paguemos un costo mayor por el trámite de un documento o servicio.

Es el viejo truco de "copia y pega", que lleva años funcionando en la Internet y que sigue tendiendo trampas a miles de personas en el mundo con páginas fraudulentas, incluso tienen los mismos anuncios del explorador de Google o Microsoft, ya que los diseños no dejan escapar el más mínimo detalle para facilitar en engaño.

Entonces, ¿qué hacer?

1. En primer lugar, verificar siempre que la URL sea la correcta y que haya un pequeño símbolo de candado en la parte izquierda de la dirección web. Es importante revisar la gramática y ortografía para no dejar pasar ningún error que pueda confundirnos.

2. Comprobar si es un anuncio. Al buscar a través de Google u otro motor de búsqueda un sitio oficial, se deben revisar detalladamente aquellos vínculos que están en la sección de anuncios pagados, en la parte superior de las páginas de resultados, ya que éstos pueden ser falsos, usualmente los sitios bancarios o de las organizaciones gubernamentales no se encuentran en esta sección.

3. Tomarse su tiempo. Antes de dar clic en el primer resultado de la búsqueda, hay que revisar todos los resultados que se obtuvieron, para identificar aquellos que son oficiales y descartar los que causen dudas. Cuando se trata de operaciones bancarias o trámites en línea, las prisas pueden ser contraproducentes.

4. Leer la página de inicio. Hay que tomarse dos minutos para revisar la página web. No hay que llenar los formularios de solicitud o transferencias bancarias, sin antes de leer el texto completo. A veces, los sitios web indican que no son los oficiales; en otras ocasiones, se encuentran errores obvios de redacción y ortografía, que nos indican que estamos ante un sitio falso.

5. Comprueba la dirección web. Que las páginas web acaben en .org o .edu no garantizan que sea oficiales. Se tiene que revisar dos veces aquellos sitios que no acaben con .mx o que tengan terminaciones de otros países, ya que pueden ser no oficiales o apócrifos.

6. https vs http. Si se ingresa información personal en un formulario o se realizan transacciones bancarias, el sitio web debe comenzar con "https" y tener el símbolo del candado, lo cual nos indica que los datos sensibles están protegidos con una comunicación encriptada, a diferencia de cuando solo es "http", para datos públicos o abiertos.

7. Al recibir un correo que anuncia la suspensión o bloqueo de tu cuenta, hay que contactar directamente al banco para confirmar que se trata de un anuncio legítimo.

8. Evita seleccionar el vínculo o link que se encuentra dentro del correo electrónico. Para ingresar a la página de tu institución bancaria o de la dependencia de Gobierno, escribe directamente en el navegador la dirección completa.

9. Los bancos y las dependencias no solicitan información personal a través de correos electrónicos. Los comunicados legítimos mediante esta vía son únicamente informativos.

En caso de ser víctima de un fraude

Lo más importante es la prevención, pero para los casos en que exista un fraude, se recomienda denunciar el sitio web fraudulento a través de los siguientes medios:

1. En Google, lo puedes denunciar en el siguiente vínculo http://bit.ly/2iaiRWa.

2. A nivel federal puedes hacer una denuncia formal a la Comisión Nacional de Seguridad:

    a. Vía telefónica: 088 (24 horas del día / 365 días del año)
    b. Correo electrónico: ceac@cns.gob.mx
    c. Vía Twitter: @CEAC_CNS
    d. Vía Web: http://www.cns.gob.mx/CNDDefWeb/pageflows/CND/denuncia.do

3. En la Ciudad de México en la Secretaría de Seguridad Pública:

    a. Vía telefónica: 52425100 EXT. 5086 (24 horas del día / 365 días del año)
    b. Correo electrónico: policia.cibernetica@ssp.df.gob.mx
    c. Twitter: @UCS_CDMX #CiberneticaCDMX

4. Con la institución bancaria de la tarjeta con que se realizó la operación, ahí nos darán instrucciones de cómo realizar la denuncia y en algunos casos se puede solicitar la devolución del monto defraudado.

Referencias Bibliográficas:

- Policía Federal. (10 de julio de 2016) *Alerta sobre páginas Web apócrifas que recolectan información personal utilizando nombres de bancos*. Gob.mx. Consultado electrónicamente el 6 de enero de 2017, 13:04 horas en http://bit.ly/2iRmlvz.

- Lucía Blasco. (13 de diciembre de 2016) *Cómo detectar las páginas Web falsas que simulan ser sitios oficiales para estafar a los internautas. BBC mundo.* Consultado electrónicamente el 2 de enero de 2017, 19:00 horas en http://bbc.in/2jkNfSL.

- Mattica. (27 de julio de 2016) *Cómo denunciar delitos cibernéticos en México*. Mattica. Consultado electrónicamente el 9 de enero de 2017, 17:05 horas en http://bit.ly/2jmO7lS.

Este documento fue elaborado por el **Mtro. Arturo Valdés,** Coordinador de Tecnologías de Información y Comunicaciones, en la Junta de Asistencia Privada del Distrito Federal.

Contacto
Martes de Tips
Katya Butrón Yáñez,
Tel. 5658 5897 ext. 8014,
kbutron@jap.org.mx