GOBIERNO DE LA CIUDAD DE MÉXICO

Junta de Asistencia Privada del Distrito Federal

No. 113
5 de marzo de 2019

MARTES DE TIPS

RECOMENDACIONES PARA REDUCIR LA INCIDENCIA Y EFECTOS DEL PHISHING

TECNOLÓGICO

El correo electrónico fraudulento o ***phishing*** son mensajes que ***intentan suplantar la identidad de otra persona o empresa***

Estos correos están pensados para confundir y así aprovecharse de los destinatarios, pidiendo algún tipo de acción a quién lo recibe, como por ejemplo solicitar donativos o depósitos a las cuentas de los estafadores, pedirnos publicar información que no es verdadera para difamar a terceros o directamente engañarnos para conseguir nuestra información financiera (números de tarjetas, nip y contraseñas) y hacer transacciones no autorizadas de nuestras cuentas.

¿CÓMO IDENTIFICO EL "PHISHING"?

El correo electrónico "phishing" se dirige a un usuario genérico, suele tener faltas de ortografía, puede estar en otro idioma, es enviado masivamente, pide información de índole confidencial y/o su remitente tiene una cuenta aparentemente confiable pero solicita la respuesta en otra cuenta distinta. Hay casos que el texto del correo va dirigido a tu nombre, pero no está relacionado con tus actividades.

Otra forma de identificarlo es por el enlace, el archivo adjunto, la acción solicitada con sentido de urgencia (pagar facturas, SAT, compra de productos) o de curiosidad (el mensaje es demasiado bueno para ser verdad como: ganar la lotería, un viaje, un premio).

PARA MINIMIZAR LA EXPOSICIÓN A ESTOS TIPOS DE FRAUDE, RECOMENDAMOS LAS SIGUIENTES ACCIONES:

- Verifica el remitente, desconfía de correos que no muestren su procedencia, de aquellos remitentes cuyo dominio sea diferente al que usualmente recibes o si presenta errores en su escritura.

- Sospecha de cualquier correo que tenga sentido de urgencia o de curiosidad y que te solicite una acción inmediata como abrir un enlace, descargar archivos o enviar datos personales.

- Pon atención en la dirección del sitio web al que te remiten, puede tener variaciones en su escritura o redirigirte a un sitio diferente al que indica.

- No abras archivos adjuntos de remitentes desconocidos.

- Es importante aclarar que ninguna institución financiera o empresa dedicada al comercio electrónico, te solicitará la actualización de tus datos por correo electrónico o el envío de información sensible.

- Si el correo parece legítimo, pero tienes dudas, llama directamente al remitente (persona, empresa, banco) y asegúrate que la comunicación sea cierta.

- Cualquier correo sospechoso o fraudulento que detectes, agrégalo a tu lista de correos no deseados, para evitar engaños futuros.

- Darse un tiempo para leer cada comunicación, ya que muchos problemas se presentan por las prisas en la que vivimos. Por ellos, es importante tomarse su tiempo para revisar a detalle la información, quién realmente la envía y por cuál razón, más cuando hay algo crítico que hacer o resolver, o que pueda afectar a más personas en su integridad y su patrimonio.

- En general, no respondas a un correo que te parece sospechoso.

PARA INCREMENTAR EL USO SEGURO DEL CORREO ELECTRÓNICO TE DEJAMOS ALGUNAS RECOMENDACIONES A SEGUIR:

- **Verificar los destinatarios de los correos electrónicos antes de enviar el correo.** Es común que la función "autocompletar" esté activa y se almacenen destinatarios falsos o fraudulentos de las comunicaciones con los correos apócrifos que recibimos. Por esta razón es necesario tomarse el tiempo de verificar los destinatarios de los mensajes que elaboremos, en especial de aquellas comunicaciones relevantes dirigidas a nuestros Donantes, Entidades de Gobierno o Aliados.

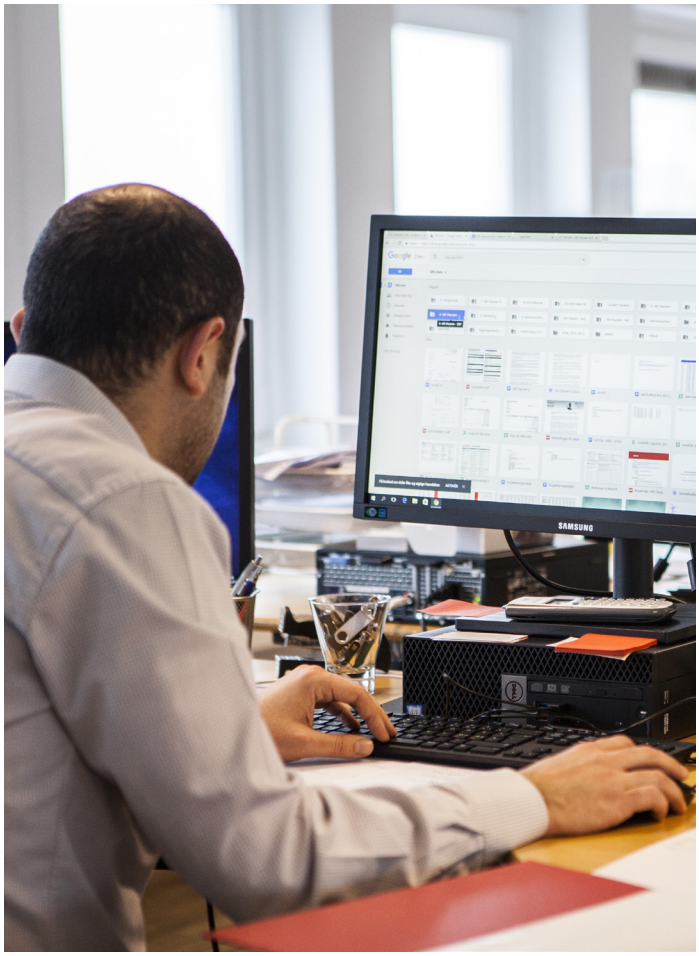
- **No utilizar el mismo nombre en el remitente** de la cuentas de correo de nuestra Organización y de nuestras cuentas personales.

- **Usar siempre una firma al pie de los mensajes que redactamos, identificando desde qué dispositivo enviamos el mensaje** (celular, laptop, tableta) y utilizando una "firma empresarial" para nuestra Organización. Con esto nuestros destinatarios se acostumbrarán a ver un tipo de firma de nuestros mensajes siempre y desconfiarán de alguien que envía un correo genérico para suplantar nuestra identidad.

- Tener **una cuenta de correo electrónico alterna,** para recuperar otras cuentas y accesos, en caso de que alguna de nuestras cuentas (de correo, redes sociales o bancos) sea comprometida, es decir, que no podemos entrar a la cuenta y sospechemos que alguien más cambio la contraseña de acceso.

- **Nunca tener la misma contraseña para las cuentas del trabajo y para las cuentas personales**, incluso, diferentes contraseñas para cada servicio que usemos, en especial los bancarios.

- **Usar contraseñas robustas, que sean difíciles de adivinar,** que combinen letras, números y símbolos y tener al menos 8 caracteres de extensión.



REFERENCIAS:

- Romo, Fabián. (Enero, 2019) Recomendaciones para reducir la incidencia y efectos del correo electrónico phishing. DSSI DGTIC UNAM. Consultado electrónicamente el 31 de enero de 2019, 14:03 horas en *https://www.tic.unam.mx/noticias/2019/01/2019-01-24-reducir-pishing.html?platform=hootsuite.*

- UNAM-CERT. (18 de enero, 2019) ¿Qué es el phishing? UNAM-CERT. Consultado electrónicamente el 31 de enero de 2019, 14:55 horas en *https://www.seguridad.unam.mx/que-es-el-phishing-2.*

ESTE DOCUMENTO FUE ELABORADO POR:
Arturo Valdés, Coordinador de la Dirección de Tecnología de Información y Comunicación de la JAPDF
Tel. 5279-7270 ext.7287 • avaldez@jap.org.mx

CONTACTO MARTES DE TIPS:
Katya Butrón Yáñez
Tel. 5658 5897 ext. 8014 • kbutron@jap.org.mx