



CDMX
CIUDAD DE MÉXICO

Ciudad de México, a 10 de mayo de 2016

ALERTA PREVENTIVA CONTRA LA CIBERDELINCUENCIA No. 40

“FRAUDE NIGERIANO”

La Secretaría de Seguridad Pública del Distrito Federal, de conformidad con las atribuciones que tiene conferidas en los artículos 3º, fracciones I, IV y V de su Ley Orgánica, 1, fracción II, y 15, fracciones I y II de la Ley que Regula el Uso de Tecnología para la Seguridad Pública del Distrito Federal, así como en los artículos 3 y 14, fracción IV de su Reglamento Interior de la Secretaría, relativas a realizar en el ámbito territorial y material del Distrito Federal las acciones dirigidas a salvaguardar la integridad y patrimonio de las personas, prevenir la comisión de delitos e infracciones a las disposiciones gubernativas y de policía, así como preservar las libertades, el orden y la paz públicos.

Situación:

Debido a la proliferación de correos electrónicos de remitentes desconocidos, en donde se ilusiona a la víctima con una fortuna inexistente y persuadiéndola a que pague una suma de dinero por adelantado como condición para acceder a la misma, cabe señalar existen diferentes variantes de Fraude Nigeriano, es por eso que la Policía de Ciberdelincuencia Preventiva de la Secretaría de Seguridad Pública de la Ciudad de México, realizó la siguiente "Alerta de Ciberdelincuencia" a fin de informar las medidas preventivas y de seguridad, ligadas al Fraude Nigeriano.

Descripción:

Las vías de contacto es por medio de correos electrónicos de remitentes desconocidos (extranjeros), en donde indican al destinatario es poseedor de una herencia, una cuenta bancaria abandonada, una lotería que ha ganado, un contrato de obra pública o simplemente una gran fortuna que alguien desea donar generosamente antes de morir.

Modo de operación:

Los timadores envían algunos documentos con sellos y firmas con aspecto oficial, normalmente archivos gráficos adjuntos a los mensajes de correo electrónico, una vez que la víctima se ha enganchado le piden datos de una cuenta bancaria con el objeto de transferir a ella grandes sumas de dinero que desean sacar del país de origen.

A medida que prosigue el intercambio se pide a la víctima que envíe dinero, con la excusa de supuestos honorarios, gastos, sobornos, impuestos o comisiones que se deben de pagar; una vez realizados los depósitos nunca llegan los traspasos, pues las millonarias sumas de dinero jamás han existido.

Recomendaciones:

- Haga caso omiso de correos electrónicos desconocidos, sobretodo de remitentes extranjeros, márkuelos como correo no deseados (spam).
- No proporcione información personal (nombre, dirección, teléfono, números de cuenta, etc).
- No realice ningún depósito por honorarios, gastos, sobornos, impuestos o comisiones con motivo de recibir traspasos de grandes sumas de dinero.
- Nadie regala nada sin motivo alguno.

“Si está tentado de responder a un ofrecimiento de este tipo, deténgase y hágase dos preguntas importantes: ¿Por qué un perfecto desconocido lo elegiría a usted? y ¿Por qué usted debería compartir su información personal con un extraño?”

