CONSEJOS PARA EVITAR LAS ESTAFAS CIBERNETICAS "PHISHING" POR MEDIO DE CORREOS ELECTRÓNICOS

DE LA JUNTA DE PROTECCIÓN AL CONSUMIDOR DEL ESTADO DE NUEVA YORK

Los correos electrónicos "**phishing**" (también referidos como "pharming" o "whaling") engañan al público pidiendoles dinero, información personal tal como números de tarjetas de credito, contraseñas o claves secretas y números de Seguro Social y esta informacíon es usada por personas no autorizadas para cometer delitos de robo de identidad.

SIGA ESTOS PASOS PARA EVITAR SER VÍCTIMA DE ESTE FRAUDE :

NUNCA:

- Responda a los correos electrónicos, pedidos por teléfono, rifas o concursos de lugares que no reconozca.
- Conteste advertencias de correos electrónicos que no muestran el nombre del remitente y dicen "undisclosed recipient" en la sección de las direcciones; igualmente los que dejan en blanco su nombre y solo dicen, "Estimado" o "Dear" sin ningun nombre después; ni tampoco los mensajes que tienen muchos errores de gramatica y/o Ingles confuso o extraño.
- Envie por correo electrónico información personal y confidencial incluyendo números de tarjetas de credito, cuentas bancarias, contraseñas, números de Seguro Social, etc. La mayoría de los correos electronicos por Internet **NO** son seguros.
- Confie en los correos electrónicos que se vean legítimos a pesar de que contienen logotipos, fotografias, derechos de autor o nombres de negocios legítimos.
- Responda a correos electrónicos, o mensajes o pop-ops pidiendo información personal o financiera.
- Haga clic en los enlaces que vienen en correos electrónicos desconocidos los cuales pueden conectarlo con sitios web sospechosos.
- Actualize su información personal a pedidos de un correo electrónico.
- Recorte y pegue enlaces de mensajes desconocidos en su buscador. Estos enlaces dan la apariencia de ser legítimos pero son diseñados para obtener información.
- Responda a grabaciones de presuntos negocios o agencias de gobierno que le dejan un mensaje telefónico pidiendo que los llame para actualizar su información. "Phishing" también ocurre por teléfono. Usando tecnología telefónica cibernetica, estafadores piden información personal y la roban.

SIEMPRE:

- Instale, actualize y utilice los programas de computadoras anti-virus y anti-espía, y los servidores de seguridad para reducir el número de correos electrónicos "phishing" que recibe. Los servidores de seguridad son especialmente importantes con conecciones de alta velocidad por lo que las computadoras están expuestas a la red de Internet desde el momento en que se prenden. Visite el sitio onguardonline.gov o staysafeonline.org para aprender más acerca de cómo proteger su computadora.
- Revise las declaraciones financieras tan pronto como usted las recibe para verificar que no haya cargos no autorizados.
- Revise su informe de crédito regularmente. Esto puede ser hecho sin cargo tres (3) veces al año por las tres (3) agencias de informes de crédito disponibles por el internet en: annualcreditreport.com.
- Use cautela al abrir cualquier archivo adjunto o bajar cualquier documento proveniente de correos electrónicos recibidos, aún de grupos conocidos, para evitar la posibilidad de infectar la computadora con un virus, un programa malicioso, u otro programa de computadora diseñado para perjudicar la seguridad de su computadora.
- Busque el prefijo de "https" y un candado cerrado antes de dar información financiera para transmisiones electrónicas por el Internet.
- Comuníquese con organizaciones o instituciones con quien usted hace negocios para averiguar sobre los correos electronicos recibidos que utilizan el nombre de la compañía. Llame al número escrito en las declaraciones oficiales de la compañía.
- Reporte estafas de phishing al spam@uce.gov, a la CPB en nysconsumer.gov, y a la institución o la compañía usada en el correo de phishing. Usted también puede reportar correos electronicos de phishing al grupo anti-phishing al reportphishing@antiphishing.org.
- Actue inmediatamente si usted proporcionó información personal a partidos desconocidos o sin verificación notificando a las compañías con quien usted tiene las cuentas y colocando un congelamiento de seguridad o alarma de fraude en sus informes de crédito con las agencias de informes de crédito.