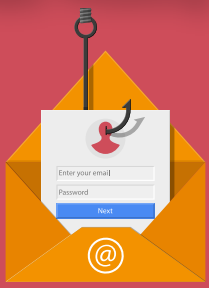
ALERTA SOBRE LAS ESTAFAS:
Suplantación de Identidad "Phishing"

Procurador General de Arizona,
Mark Brnovich



Detalles sobre las estafas:

Los fraudes de suplantación de identidad o phishing son diseñados para robar su información personal, generalmente a través de correo electrónico. Estos correos electrónicos fraudulentos parecen ser de una empresa de confianza pidiéndole su número de Seguro Social, el número de su tarjeta de crédito, o su nombre de usuario y contraseña. La nota electrónica le pedirá la información directamente o le instará para que usted visite un sitio web o que llame a un número telefónico, en el cual los estafadores se hacen pasar por una compañía legítima.

Recuerde que una empresa legítima no le pedirá su información por medio de correo electrónico.

Señales de Advertencia:

- La nota electrónica expresa urgencia para que usted entregue información sensible o haga un pago.
- Ofertas no solicitadas o peticiones de información personal por correo electrónico que parecen representar a una compañía, agencia, o institución financiera de confianza.
- Encabezados vagos o un saludo genérico, tal como "Hola Cliente".
- Notas electrónicas con mala gramática o secuencia ilógica en las oraciones.
- Una nota electrónica solicitando su número de Seguro Social u otra información de identificación personal.
- Una nota electrónica que le pide a usted que abra un adjunto.

Protéjase:

- No haga clic ni abra enlaces en notas sospechosas de correo electrónico. Si usted no está seguro/a si la nota electrónica proviene de una fuente de confianza, use un buscador para obtener la información de contacto de la empresa y comuníquese con ellos directamente.
- Esté consciente de anuncios y noticias falsas en las que usted pueda hacer clic, exponiéndose a sí mismo/a a ataques de robo de identidad o programas maliciosos de cómputo.
- Si usted está navegando por la web y aparece una ventana emergente "popup" diciéndole que su computadora tiene un virus o que usted se ganó un premio, cuidado, éstas casi siempre son estafas.
- Aún si una nota electrónica o comunicación de los medios sociales provino de uno de sus mejores amigos o miembros de familia, recuerde que a ellos también se les podría haber engañado o pirateado (hackeado). Es por eso que usted debe ser prudente en cualquier situación. Incluso si un mensaje parece ser amable, trate a los enlaces y adjuntos con sospecha.
- Si usted descubre una estafa de suplantación de identidad (phishing), repórtela al banco, al departamento de apoyo de su red social, o a cualquier otra entidad que el mensaje de suplantación de identidad (phishing) afirme representar.

Recursos:

Oficina del Procurador General de Arizona
www.azag.gov/complaints/consumer
Phoenix: 602 - 542 - 5763, Tucsón: 520 - 628 - 6648
Ó larga distancia gratuita: 1- 800 - 352 - 8431

Línea de Ayuda de la Fuerza de Trabajo Contra el Abuso de Personas Mayores
602 - 542 - 2124 ó 1- 844 - 894 - 4735

www.azag.gov/seniors/scamalert