

Fecha 04.08.2020	Sección Ciudad	Página 3
----------------------------	--------------------------	--------------------

Advierten por aumento de ciberdelitos

Roban información con correos falsos

Obtienen los datos **bancarios** a través de mensajes apócrifos de las **empresas**

ARIADNA LOBO

Los correos electrónicos falsos de **empresas** formales se han vuelto un método cada vez más frecuente que usan los ciberdelincuentes para el robo de información de los usuarios, estafas y **fraudes**.

El cierre de comercios durante la Jornada de Sana Distancia provocó la migración de compradores a las redes sociales o páginas web y con ello los ciberdelincuentes recurren a prácticas en línea para hurtar datos personales y **bancarios**.

Esta práctica, también conocida como phishing, Fraude Nigeriano o Fraude 419, tiene como objetivo obtener información de los usuarios a través de correos electrónicos, que parecieran ser de **empresas** formales, pero al ver a detalle no lo son.

Por ello, la **Secretaría** de Seguridad Ciudadana (SSC)

recomendó no abrir estos correos, ni los enlaces,

“Por ejemplo, tengo mi cuenta en **Bancomer** y quiero consultar mi saldo y entro a una página o me llegan correos de **Bancomer**, y en esto consiste el phishing, que en lugar de que te llegue un correo del **banco**, te va a llegar un correo de ‘Banncomer.com’, de tal manera que no lo veas bien y pienses que sí es el **banco**.”

“Y es una página igualita y ni siquiera tiene que ser un hacker muy bueno, puede ser un programador que compre el dominio con el nombre ‘Banncomer’ y copie la página original”, explicó el experto en ciberseguridad, Hugo Galicia.

Ahora con el confinamiento, hay que tener presente que las personas que se dedican a este tipo de **fraudes** también se encuentran confinadas y con mayor tiempo para innovar en estos delitos, dijo Galicia.

Sin embargo, no sólo se realiza phishing con páginas de **bancos**, también imitan correos de **empresas** como Amazon o **Mercado** Libre pa-

ra obtener información de los usuarios, o incluso, se pueden robar datos por medio de encuestas en la calle.

“Yo me puedo poner un chalequito y decir que vengo de Unicef, que no pido dinero ni donaciones, pero que tengo unas pulseritas y sólo

necesito que me contestes unas preguntas, así empiezan a preguntar cosas como qué tipo de gatitos prefieres o cómo se llamó tu primer mascota, y con eso te sacan información que es la que usas en las preguntas de **seguridad** y al final te preguntan tu nombre”, explicó Galicia.

La usurpación de identidad también está relacionada con esta práctica de fraude, pues se comete mediante robos de información de tarjetas **bancarias** para después realizar compras electrónicas.

En lo que va del año, La Fiscalía General de Justicia tiene 972 carpetas de investigación por este delito, de las cuales 121 fueron recibidas en la Unidad de Recepción por Internet.

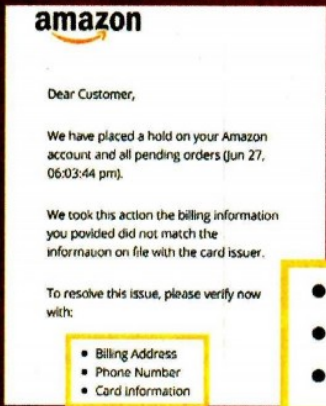


Fecha 04.08.2020	Sección Ciudad	Página 3
----------------------------	--------------------------	--------------------

Lanzan anzuelo

En los mensajes solicitan se proporcionen datos personales y bancarios.

En mensajes apócrifos los pequeños detalles en tipografía u ortografía los distinguen de los originales.



amazon

Dear Customer,

We have placed a hold on your Amazon account and all pending orders (Jun 27, 06:03:44 pm).

We took this action the billing information you provided did not match the information on file with the card issuer.

To resolve this issue, please verify now with:

- Billing Address
- Phone Number
- Card Information

Amazon.com

otro
suscripción...@amazon.com...
Agregar a lista VIP
Bloquear este contacto

Hugo Galicia, experto en ciberseguridad

// Es una página igualita y ni siquiera tiene que ser un hacker muy bueno, puede ser un programador que compre el dominio con el nombre 'Banncomer' y copie la página original".