Ciberestafas: 1 de cada 3 mexicanos caen en correos falsos

Posted on 7 de enero de 2021 by Diario Humano

Una investigación de Kaspersky también reveló que, en caso de recibir un mensaje sospechoso en el celular, los latinos son más cautelosos para las ciberestafas

Diario Humano | La Paz, Baja California Sur

El phishing o robo de identidad es una de las **ciberestafas más comunes.** Mediante este método, los **criminales** sustraen datos personales para acceder a **cuentas bancarias y números de tarjetas de crédito, y así defraudar a los usuarios.**

Los delincuentes utilizan diferentes vías para cometer **phishing**, la más utilizada continúa siendo el **correo electrónico,** simulan ser mensajes de **entidades oficiales**; incitan a los destinarios a hacer clic en enlaces o abrir archivos maliciosos.

A menudo, instituciones públicas y privadas alertan sobre la difusión de **correos sospechosos** para que las personas eviten caer en este tipo de ciberestafas.

Una investigación desarrollada por la compañía global de ciberseguridad **Kaspersky**, en conjunto con la consultora de estudios de mercado CORPA, reveló que, en promedio, el 38% de los latinoamericanos no sabe distinguir un e-mail verdadero de uno falso.

En ese sentido, quienes menos lo hacen son los peruanos, con un 53%. Más atrás se ubican colombianos (42%), mexicanos (38%), chilenos (35%), argentinos (32%) y finalmente, brasileños (30%).

Una cifra similar se obtuvo cuando se consultó a los usuarios qué harían si recibiesen un correo para participar por 2 pasajes con todo pago al Caribe, donde se exhibiera el logo de una importante aerolínea.

De los encuestados, un tercio (37%) desconfiaría y por ningún motivo haría clic en el enlace incluido en el e-mail; mientras un 46% dudaría y consultaría primero en internet si el concurso es o no real. En tanto, un 15% verificaría la URL y luego accedería al link.

La campaña Iceberg Digital, fue realizada por Kaspersky para analizar la situación que viven en materia de ciberseguridad los internautas en **Argentina, Brasil, Chile, Colombia, México y Perú**; y develó algunos **riesgos** que tanto empresas como usuarios comunes corren cuando **se conectan y navegan en la red crédulamente y sin cuestionamientos.**

Iceberg Digital tiene como fin prevenir que individuos y compañías sean víctimas de "icebergs digitales"; sitios web, apps, enlaces o imágenes que a simple vista se ven inocentes o superficiales, pero que en realidad esconden algo oscuro y desconocido, se "estrellen" contra ellos y acaben naufragando.

Molestia y desconfianza

El estudio evidenció además que, en el caso de recibir un **mensaje de texto (SMS)** dudoso en el celular que indique, por ejemplo, que la cuenta corriente ha sido hackeada junto con un enlace para verificar su estado; los latinoamericanos parecen reconocer mejor una eventual estafa y actúan de forma más cautelosa.

El 33% asegura borrar o ignorar estos contenidos, mientras que un 65% llama directamente al banco para verificar la información.

La investigación mostró asimismo que los usuarios de la región desconfían de los enlaces publicitarios por sospecha de que estos contengan virus o las ciberestafas; y en ese sentido, quienes más dudan son **argentinos, con 44%, y chilenos, con 42%. Más atrás se ubican brasileños (39%), mexicanos (38%), peruanos (33%) y colombianos (31%).**

"Algunos de estos correos son fáciles de detectar ya que incluyen errores ortográficos, gramática descuidada, gráficos poco profesionales, y saludos demasiado genéricos.

Sin embargo, se han detectado correos más sofisticados que son capaces de engañar hasta a los usuarios más cautelosos. Por eso, es importante permanecer alerta y no bajar la guardia.

"Especialmente al recibir correos o mensajes que parecen provenir de entidades oficiales y comunican una urgencia; como una oferta disponible a un número limitado de usuarios o amenazan al destinario con multas, si este no toma la acción requerida a la mayor brevedad," alerta **Roberto Martínez, analista senior de**

seguridad en Kaspersky.

“Lo mejor es desconfiar y verificar directamente con la entidad oficial; especialmente cuando esos correos incluyen archivos adjuntos o enlaces, o piden verificar la dirección de e-mail u otra información personal”.

Para lograr reconocer un correo falso de uno verdadero y evitar las redes de ciberdelincuentes y ciberestafas, Kaspersky ofrece los siguientes consejos de prevención:

Desconfíe siempre de los mensajes de correo alarmantes. **Las entidades de confianza, como bancos, compañías de seguros o cualquier otra empresa comercial, no solicitan datos personales ni información de la cuenta mediante el correo electrónico.**

Si en alguna ocasión recibe un e-mail con peticiones de esta naturaleza, elimínelo y llame a la empresa en cuestión para asegurarse de que no hay ningún problema con su cuenta.

Si sospecha, elimine el mensaje sin abrirlo. Algunos clientes de correo electrónico permiten scripting, lo que hace posible tener un virus simplemente al abrir un correo electrónico sospechoso. Lo mejor es que evite abrirlos.

No abra archivos adjuntos a estos mensajes sospechosos, especialmente los que vengan en formato Word, Excel, PowerPoint o PDF, ya que pueden descargar malware.

Nunca haga clic en las direcciones URL incrustadas en el mensaje original. En su lugar, visite el sitio directamente escribiendo la dirección URL correcta para verificar la solicitud y consulte los procedimientos y las políticas de contacto que sigue el proveedor a la hora de solicitar información.

Utilice una solución robusta de seguridad, **Diario Humano** recomienda **Kaspersky Internet Security,** que protege de amenazas comunes, como gusanos y troyanos, y de otras más sofisticadas, como botnets y aplicaciones maliciosas.

Además, cuenta con tecnología antimalware avanzada que bloquea adware y phishing, protege contra ciberestafas financieras, ransomware, y otras ciberamenazas.