No te dejes enganchar

Al hablar de Phishing, ¿qué te viene a la mente? Normalmente estamos familiarizados con términos en inglés pero quizá por su origen y forma de escribir no entendemos algunos ni los tomamos en cuenta.

Alguna vez al pagar un servicio, ¿la cajera te ha comentado que tu tarjeta no pasa o no tienes ni un peso en tu cuenta? Si no lo has vivido, seguro has escuchado sobre algún caso parecido.

¿Qué pudo haber pasado? Quizá te gusta realizar compras en línea pero, ¿te fijaste que el sitio fuera seguro? o ¿tu banco te mandó un correo electrónico para revalidar tus datos personales y llenaste el formato sin pensar ni consultar con alguien de esa institución?

Es probable que hayas proporcionado información de tu cuenta bancaria o número de tarjeta de crédito a través del *Phishing,* que es una forma de estafa virtual en la cual tus datos fueron recabados para utilizarse de manera fraudulenta.

Es importante mantener la confidencialidad de tus datos y si te piden proporcionarlos, siempre revisa que lo estés haciendo por un medio seguro. Pasa de largo los anzuelos y protege tus cuentas de esta manera:

NO ACEPTES CUALQUIER MENSAJE

A veces al consultar páginas en internet, salen anuncios a los cuales no les tomas importancia, incluso no los lees, pero como son molestos, quizá das clic en un botón de aceptar sin saber que estás consintiendo la instalación de algún programa que permita robar tus claves.

REVISA LA AUTENTICIDAD DE LAS PÁGINAS DE INTERNET

Las páginas donde realizas compras son muy llamativas, y la emoción por adquirir algo al instante, puede distraerte de poner atención en la seguridad del sitio consultado. Eso lo saben muy bien quienes pretenden adquirir tus claves de tarjeta o cuentas bancarias. Siempre asegúrate que la página sea auténtica, ¿cómo? Revisa que empiece con **"https://"** y un pequeño candado cerrado en la barra del navegador. Incluso algunas páginas te permiten dar clic sobre el icono para visualizar el certificado de seguridad y comprobar su validez. Puedes notar que tratan de timarte cuando aparece la página exactamente igual a como siempre la ves, pero la dirección electrónica no tiene nada que ver.

Siempre observa esos detalles, sé prudente al poner tus datos en un formulario pues no sabes si en realidad "la oferta que estás aprovechando" te robará más que el descuento increíble que encontraste.

EN TU CORREO

Es habitual la creación de correos electrónicos falsos que aparentan proceder de una institución financiera y pretenden engañar a los clientes de la misma. En ellos te piden que ingreses tus datos para corroborar que efectivamente eres usuario, para que accedas a algún beneficio o reactives un servicio. Son correos peligrosos porque imitan el aspecto y funcionalidad, ya sea total o parcial de la propia institucion financiera, por lo que pocas veces generan duda en el interesado.

¿TRANSACCIONES BANCARIAS?

Seamos honestos, queremos evitar a toda costa el trayecto al banco y la desesperante fila de clientes, por lo que buscamos realizar movimientos bancarios a través de nuestra computadora o celular. ¡Ojo! Es una de las formas más sencillas que tienen los criminales cibernéticos para robar tu información. Asegúrate que el sitio *web* consultado sea el oficial de tu banco.

POR ENTRETENIMIENTO

No utilices enlaces que para acceder a sitios web te pidan información confidencial. En su lugar, te recomendamos escribir en el navegador la dirección correspondiente.

PROTÉGETE

Te recomendamos tener un programa antivirus instalado y actualizado en tu computadora, siempre revisar que la página consultada sea segura y no fiarte por la apariencia del sitio que visitas. Mantén protegidos tus datos y seguro tu dinero.