Cómo evitar ser víctima de Phishing:

Profeco alertó sobre este fraude para para robar información

mexus®
Managed secure IT | no matter what

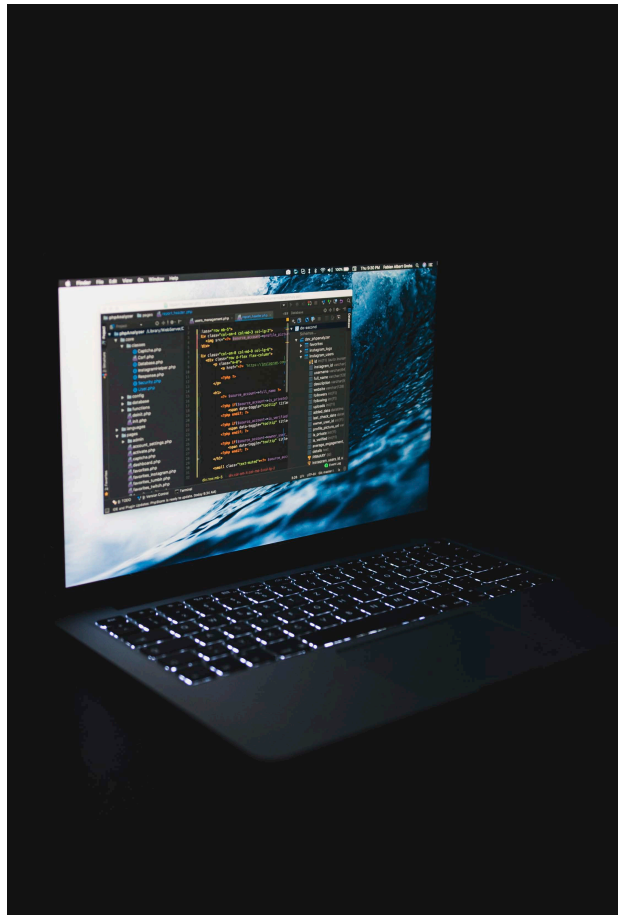
Cómo evitar ser víctima de Phishing:

Profeco alertó sobre este fraude para para robar información

Este tipo de ataques son muy comunes pero también fáciles de evitar si se tiene la información correcta.

La Procuraduría Federal del Consumidor *(Profeco),* alertó a la población de México sobre el Phishing, uno de los tipos de fraudes más comunes y que puede ser frenado a tiempo para evitar el robo de información.

En el marco del Día del Internet Seguro, la dependencia señaló que dicha actividad se realiza a través de mensajes de texto, llamadas y correos electrónicos.



¿Qué es el phishing?

De acuerdo con Profeco, se trata de un tipo de ***fraude digital que suplanta la identidad.***

Este se realiza por mensajes de texto, llamadas y con mayor frecuencia por correo electrónico, con el objetivo de ***robar información personal, dinero o provocar que se descargue un virus.*** Este tipo de amenazas también pueden buscar tomar el control del dispositivo o computadora.

¿Cómo reconocer el phishing?

Este tipo de fraude en línea ***se realiza a través de mensajes que parecen enviados de compañías conocidas*** ya que pueden tener el mismo aspecto. Frecuentemente cuentan ***una historia para enganchar y lograr que la víctima haga clic en un enlace.***

Algunos de los métodos que ocupan son:

. Señalar que se ha detectado una actividad sospechosa e intentos de inicio de sesión

. Afirmar que hay un problema con la cuenta o la información de pago

. Decir que se deben confirmar algunos datos personales

Este tipo de fraude en línea se realiza a través de mensajes que parecen enviados de compañías conocidas (Foto: Europa Press)

¿Cómo se puede evitar este tipo de estafas?

Para evitar caer en un fraude como el phishing se debe de ***reforzar la seguridad en dispositivos electrónicos y navegación,*** por ejemplo:

. Utilizar el sistema de verificación en dos pasos en cuentas.

. Comprobar que la URL de los sitios web empiezan con ***"https".***

. ***Desconfiar de ofertas increíbles*** o que ofrecen formas rápidas de ganar dinero.

. Recordar que sitios web legítimos no solicitan por mensajes contraseñas o información financiera.

. Utilizar una ***solución de seguridad completa*** y confiable para estar protegido.

. Contar con el ***software actualizado.*** De esa manera uno se asegura de que el sistema operativo cuenta con los parches o correcciones necesarios para estar protegido ante eventuales ataques.

. ***Evitar la conexión WiFi pública,*** sin protección de contraseña y donde todo el tráfico pueda quedar expuesto. Lo ideal es utilizar una VPN confiable para conectarse, sobre todo si se va a ingresar datos confidenciales en la web.

Con la pandemia han aumentado los fraudes a distancia.

¿Qué otras amenazas son comunes?

De acuerdo con la Secretaría de Comunicaciones y Transportes, otras de las ***tácticas más usadas*** son: ***Smishing y Vishing,*** con estas los criminales de ingeniería social también intentan engañar a las personas para que revelen información confidencial o realicen ciertas acciones como ejecutar archivos que parecen ser benignos, pero que en realidad son maliciosos.

. ***El Smishing*** ocurre cuando se recibe un mensaje de texto corto (SMS) al teléfono celular, por medio del cual se solicita al usuario llamar a un número de teléfono o ir a un sitio web.

. ***El Vishing*** es la estafa que se produce mediante una llamada telefónica que busca engañar, suplantando la identidad de una persona o entidad para solicitar información privada o realizar alguna acción en contra de la víctima.

La capacidad de identificar un ataque de ingeniería social minimiza, en gran medida, el ***riesgo de ser víctimas de los ciberdelincuentes*** y ver comprometida información. Para ello, se recomienda preguntarse antes de abrir cualquier enlace, archivo anexo, mensaje de texto o llamada de un remitente desconocido: si estaba esperando esa información, si reconozco el remitente, o si solicitan hacer algo y poner en duda a aquellos que no coincidan con lo esperado.

La pandemia ha desencadenado un aumento del cibercrimen a todos los niveles. Los desafíos de ciberseguridad seguirán existiendo. ***Ciberdelincuentes*** y grupos organizados aprovecharon los meses de desconcierto global para desplegar nuevos métodos y vectores de ataque. Las cifras hablan por sí solas: en marzo los ciberataques relacionados con el Covid-19 alcanzaron el pico de un millón al día y se produjo un aumento del 30.000% en phishing, sitios web maliciosos y malware dirigido a usuarios remotos.

Fuentes de información:
https://www.infobae.com/