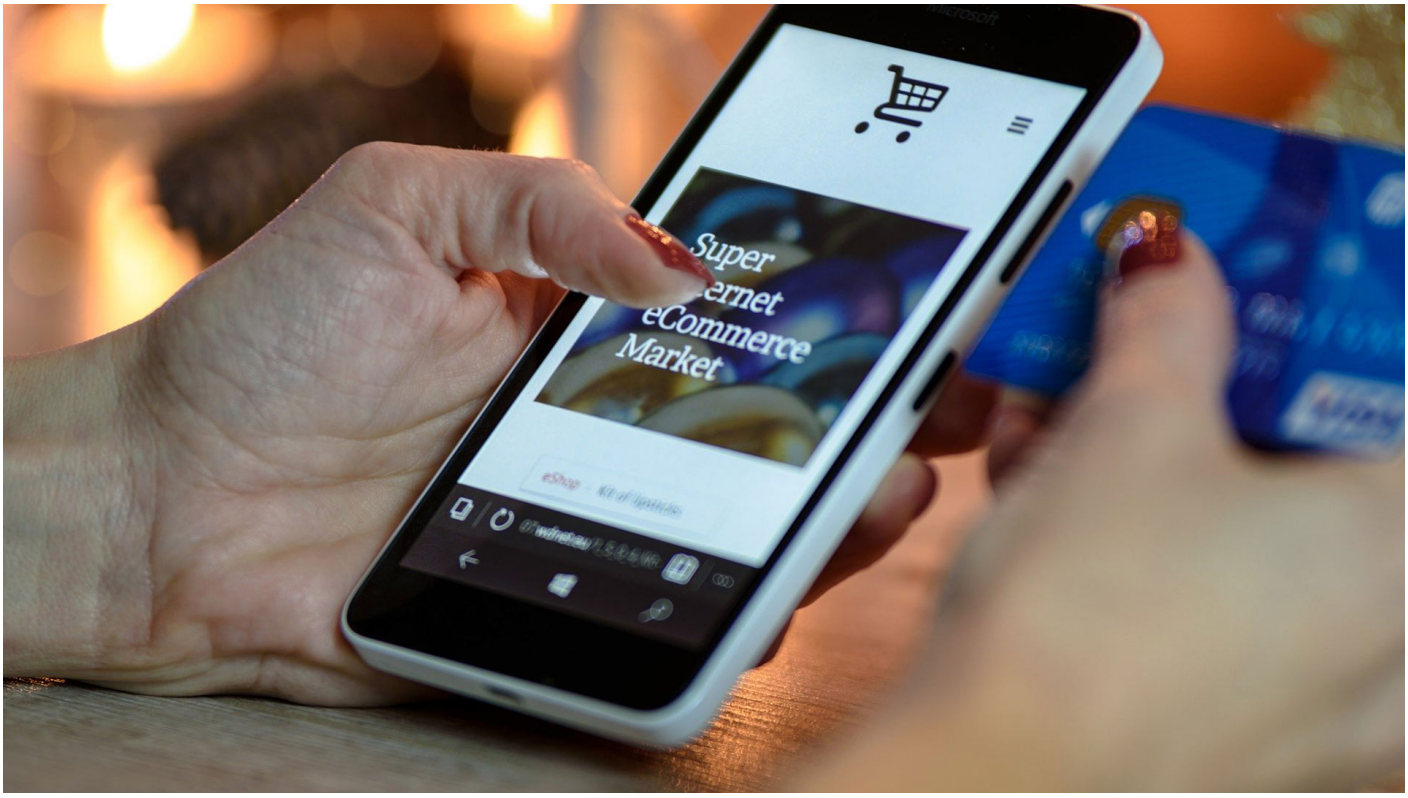
Consejos de ciberseguridad para compras en línea ante el COVID-19



Ante la pandemia de **COVID-19** que se vive actualmente en el mundo, toda la atención está centrada en la **emergencia de salud mundial,** abriendo así una puerta a los hackers, quienes pueden aprovechar para vulnerar **los sistemas de las instituciones financieras,** advierten analistas.

Félix Barrio, director del **Hub Ciberseguridad del Tec de Monterrey,** habla sobre cómo evitar los **ataques cibernéticos** en opciones de pago en línea con instituciones financieras o proveedores de servicios ante esta pandemia.

“Ahora mismo estamos asistiendo a una oleada de ataques que están intentando aprovecharse de la situación de pánico general que hay en los países en torno al tema del Coronavirus, ***COVID-19,***

“Las organizaciones financieras y las empresas está siendo víctimas de un creciente número de ataques, pero también, se están viendo ***muchas campañas para engañar directamente a los usuarios,*** *con páginas falsas que se hacen pasar por entidades que realmente no lo son, con intención de hacer algún tipo de fraude”, compartió.*

El especialista refiere que las **instituciones financieras** ya se encuentran tomando medidas y lanzando alarmas para que la población **tome precaución en este sentido.**

“Lo que están haciendo ahora las entidades financieras, en su mayor parte es recordar a los usuarios que ***nunca les van a pedir determinados datos personales y financieros ni por correo electrónico, ni sistemas de mensajería, ni mucho menos por teléfono,***

“Aunado a concientizarlos para que no sean víctimas de ese tipo de fraudes que pueden recibir pidiéndoles determinados datos con la excusa de que se han bloqueado las cuentas, algún tipo de movimiento u operación no identificada en sus tarjetas, etc”, enfatizó.

Como usuarios ante estos ataques que podemos sufrir **al comprar o pagar en línea debido al aislamiento impuesto por el COVID-19,** el especialista en **ciberseguridad** da una serie de consejos sobre **cómo podemos protegernos.**

“Lo primero sobre todo, es tener mucha precaución cuando accedemos a nuestras plataformas financieras, así como cuando hacemos transacciones económicas en portales de compras”, destacó.

1. Conectarse a un WiFi privado

“Si el Wifi al que estás conectado no es privada, no nos conectemos a páginas web de nuestros bancos o plataformas de comercio electrónico, a menos que sea a través de una conexión cifrada, VPN,

“Esto nos permitirá que naveguemos en la red abierta de internet sin que un tercero nos esté espiando nuestro tráfico y conexión privada a las transacciones que hagamos de tipo financiero”, puntualizó.

2. Instalar un antivirus en equipos móviles

“Cuando accedemos desde el dispositivo móvil a nuestros datos bancarios o hacemos una transacción, tenemos que asegurarnos que ese dispositivo no tenga ningún tipo de software espía,

“Eso se evita teniendo instalado un antivirus en el dispositivo desde el que hacemos consultas en las instituciones financieras”, aseguró.

Los **smartphones** son la principal fuente de **transmisión de malware** (software que puede comprometer el equipo o la información del usuario) pues representan el 60% de esta actividad, por delante las computadoras y laptops.

Sin embargo, los usuarios no tienen el hábito de instalar aplicaciones antivirus en sus celulares, a pesar de que hay muchas opciones, que evitan contribuir a la proliferación de estos **softwares maliciosos**.

Los ataques cibernéticos **se aprovechan de los usuarios que no actualizan el software** de sus computadoras, laptops o celulares.

*“La mayoría de los usuarios por desgracia, tiene instalado un antivirus en su computadora de escritorio, pero **muy pocos somos los que lo tenemos instalado en nuestro smartphone o en nuestra laptop,***

“Este es un lugar donde los ciberdelincuentes está siendoles más fácil el instalar este tipo de virus informáticos que lo que hacen es capturar nuestras contraseñas, datos bancarios y espiar nuestras comunicaciones”, destacó.

3. Desconfiar de correos virales que hacen algún tipo de oferta

"Tenemos que desconfiar cuando nos llegan correos virales que hacen algún tipo de oferta, ***es importante rechazar estos correos que se están haciendo pasar por bonos o vales de oferta con motivo de la crisis*** *ocasionada por el* ***COVID-19",***

El pasado 25 marzo salió una campaña falsa de un lugar que se hacía pasar por la plataforma de streaming **Netflix,** -te ofrecía una cuenta gratuita durante la crisis y realmente te conducía a una página web falsa de **Netflix** donde te pedían tus datos para que pudieran luego hacerte algún tipo de acceso a tus datos bancarios o hacer compras en tu nombre- cuenta el especialista.

"Por lo tanto, ***tengan mucho cuidado cuando lleguen este tipo de correos virales,*** *de no acceder sin fijarnos muy bien que la página de web no sea sospechosa, que el dominio de la barra de direcciones donde está esa aplicación tenga su candado verde y* ***que empiece por las letras https: que indica que es un lugar seguro"****, puntualizó.*

width="1920" loading="lazy">

El director del **Hub Ciberseguridad del Tec de Monterrey,** pide a la población **estar alerta de este tipo de engaños y reportarlos cuanto antes** a las instituciones financieras y proveedores de servicios.

"En definitiva, ante la mínima duda desconfiar, llamar al banco, al proveedor habitual de servicios y confirmar si ha enviado algún tipo de información o es un delincuente que se está haciendo pasar por él", enfatizó.

A dos años del ciberataque al **SPEI,** Félix Barrio, refiere que en este momento donde todo se está haciendo a través de internet como pagos en línea y teletrabajo por la pandemia de **COVID-19,** es importante la **concientización.**

"Afortunadamente, las empresas del sector financiero y los bancos, suelen estar bastante dotados de medios y capacidades, pero el hecho de que sus empleados trabajen en remoto, está

suponiendo una mayor necesidad de reforzar esa seguridad,

“Hay una mayor vulnerabilidad a ataques de ingeniería social como los que se sufrieron en el ataque de SPEI que fue un ataque muy sofisticado, en el que se comprometieron datos de empleados de las entidades.

“Por eso, para evitar que suceda ahora en este escenario de pagos en línea y trabajo remoto hay que ***reforzar toda la seguridad de la conexión y sobre todo, poner en práctica la concientización”.***

Para finalizar, el experto mencionó que **las empresas pueden evitar este tipo de ataques, al invertir en la preparación del personal.**

“Como dice IBM una de las empresas del ***Hub de Ciberseguridad del Tec****, el* ***95%*** *de los fallos de* ***ciberseguridad*** *siempre van a tener un componente humano,*

“Por lo tanto, lo que se está haciendo por parte de las empresas es ***invirtiendo en preparar a ese factor humano para que sea menos vulnerable a los ciberataques”,*** *concluyó.*

SEGURO QUERRÁS LEER TAMBIÉN: