

Queportatilcomprar.net enseña a blindar la privacidad en tu ordenador portátil frente a estafas y fraudes

La inmersión en la era digital y lo que se avecina con la tecnología blockchain hacen imprescindible la protección de la privacidad personal.

MADRID, SPAIN, January 12, 2022 /EINPresswire.com/ -- Los ataques cibernéticos son muy frecuentes y más aún con la descentralización de las finanzas DeFi. Además, la llegada inminente de la web 3.0 soportada en la tecnología blockchain va a ser un caramelo para hackers informáticos.



Web 3.0

Ni siquiera comprar uno de los [mejores portátiles](#) del mercado asegura que alguien pueda alterar nuestra privacidad. De hecho, con las nuevas organizaciones autónomas descentralizadas y la llegada de la web 3.0 en un próximo futuro, finalmente el usuario tendrá propiedad digital, esto implica un gran desafío a la hora de proteger la privacidad personal.

“

Especialistas en informática tanto software como hardware”

Pablo Chamorro

Como es obvio, el papel de los antivirus es una materia esencial en los equipos informáticos, sin embargo, este es uno de los muchos factores a tener cuenta a la hora de proteger la privacidad de los dispositivos electrónicos portátiles. [Queportatilcomprar.net](#) los expone, además de las estafas y fraudes más conocidos.

Antivirus sí o sí

Sin duda, un buen antivirus es la forma más segura de proteger la privacidad frente a infecciones cibernéticas. Los más avanzados hacen monitorizaciones en tiempo real y de manera automática si se actualizan frecuentemente.

Una red wifi segura

La red wifi más segura es la doméstica mientras esté bajo control, ya que, es aquí donde empiezan todos los caldos de cultivo de los malwares. No solo porque vecinos puedan conectarse y ahorrarse la contratación de la tarifa mensual, esta historia va mucho más allá.

Tener bajo control la vulnerabilidad de la red doméstica es un principio inmutable frente a los ataques. Ya que desde aquí pueden controlar la configuración del router, cambiar la contraseña y acceder al ordenador portátil.

Es aconsejable contar con un sistema de protección de tu red doméstica, se trata de integrar soluciones de seguridad de ESET.

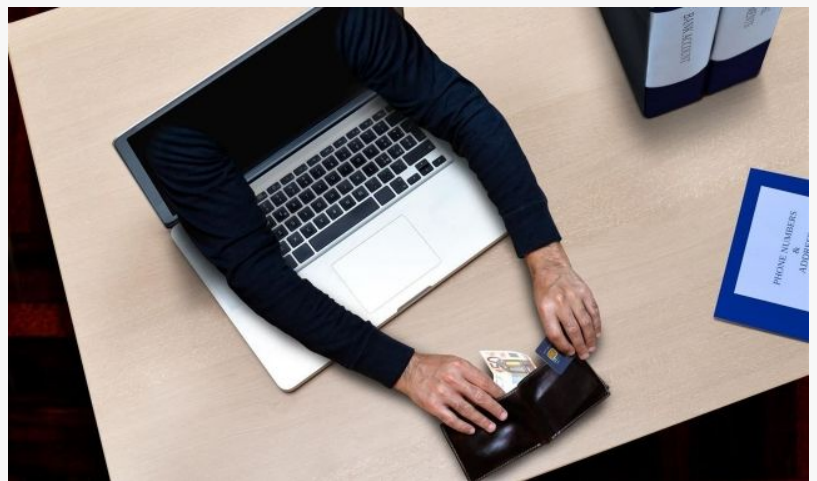
Una VPN para temas sensibles

Muchos hackers estarán atentos a las finanzas personales del usuario, ya sean índices, stocks o criptomonedas. Si consiguen el acceso a las webs donde se compran estos activos, pueden liquidar saldos en cuestión de minutos. Es por ello que es aconsejable hacerse con una VPN que está conectada a otro servidor, y desde aquí, una vez conectados empezar a operar.

Acceder solo a webs de confianza

Antes de interactuar con una web, es aconsejable observar su protocolo de seguridad, se trata del candadito que aparece justo a la izquierda de la URL en la barra de navegación, si este se mantiene cerrado, estamos ante una web que utiliza un protocolo de seguridad https (seguro y encriptado). Por el contrario, si está abierto, el protocolo no es lo suficientemente seguro como para depositar confianza en esa web y navegar a través de ella.

Muchos de los ataques cibernéticos son invisibles a los ojos, sin embargo, algunos de ellos necesitan de las acciones del usuario. En el siguiente apartado se exponen algunos de los fraudes y estafas más comunes a los usuarios.



estafas y fraudes por internet



fraudes en compras online

Estafas en compras online

La recepción de correos electrónicos ofreciendo el [mejor portátil calidad precio](#) del mercado puede salir bastante caro. Las ventas online han aumentado de manera exponencial durante la última década, de hecho, la adaptación de negocios tradicionales al medio digital ya no es una opción, sino una obligación.

Los estafadores se han dedicado a alimentarse de los fraudes online ofreciendo productos online a mitad de precio mediante el correo electrónico. Asegurarse donde hacer clic, puede ahorrar disgustos.

Fraudes Nigerianos

Así es, se le conoce como la estafa 419, anteriormente utilizada únicamente en el territorio nigeriano pero extendida internacionalmente.

Las víctimas reciben correos electrónicos donde se les ofrece grandes sumas de dinero debido a la muerte de alguien que les ha incluido en el testamento o simplemente por un sorteo. Recuerda que nadie da duros a pesetas.

Estarían a dos clicks de poder estafarte, es más, este tipo de fraude podría llegar a ser peor llegando a perpetrar delitos más graves como son los secuestros y extorsiones.

Estafa romántica

El amor conlleva muchos sentimientos encontrados y hacer pensar que conseguir a la media naranja está a la vuelta de la esquina, puede ser el desencadenante de un gran fraude.

Esto empieza por la creación de perfiles falsos en redes sociales, fotos, videos y más contenido de personas ficticias enamorando a la víctima. En el mejor de los casos, supondrá la pérdida de dinero y la decepción, sin embargo, también puede correr peligro la integridad física.

El Phishing

Se trata de la suplantación de identidad, una de las más conocidas y extendidas en internet. Este tiene que ver con la situación financiera, tratando de robar las credenciales de acceso a los servicios bancarios, o cualquier otra información relevante.

Como se comenta anteriormente, existen sistemas de protección informática como ESET que integran soluciones de detección y bloqueo del ataque antes de que puedan perpetrar tu equipo informático.

Pablo Gómez Chamorro
Queportatilcomprar.net
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/560325245>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 IPD Group, Inc. All Right Reserved.