Aprende a mejorar la seguridad en Internet este 2024

La seguridad y la privacidad siempre es importante para cada ser humano, no obstante, en este mundo global, es muy difícil mantenerla.

Las amenazas cibernéticas siempre están a la orden del día y tu información personal puede verse perjudicada, no obstante, existen algunos trucos que pueden ayudarte a mantener seguro tu internet para este año.

Según el portal MuyComputer, el número de amenazas a nivel del cliente ha aumentado con todo tipo de malware; campañas de bulos y desinformación; pérdida del derecho a la privacidad o vulnerabilidades de software no parcheadas que son explotadas en ataques de Ransomware y Phishing, sin duda los más peligrosos.

Por eso, protege tus datos con estos simples pasos:

- **Protege los navegadores web**: Todos los navegadores incluyen características avanzadas de seguridad cuya activación debemos revisar y configurar porque son las aplicaciones principales que usamos para acceder a Internet y a sus servicios.

Además de revisar el cifrado de extremo a extremo en la sincronización o el aislamiento de procesos (*sandbox*), debemos prestar atención a los avisos sobre sitios inseguros que muestran los navegadores.

También revisar las extensiones instaladas porque algunas son una fuente frecuente de introducción de malware.

- **Actualiza el sistema operativo y aplicaciones**: Cualquier tipo de software es susceptible a vulnerabilidades que los ciberdelincuentes aprovechan para los ataques informáticos. De ahí la necesidad de usar siempre las últimas versiones del software que utilicemos, especialmente de los sistemas operativos. Todos tienen mecanismos para ello y en el caso de Windows, el más utilizado y explotado, cuenta con Windows Update para proporcionar actualizaciones automáticas que facilitan su parcheo y actualización a las últimas versiones. Si tienes experiencia y prefieres hacerlo manualmente, Microsoft

Update Catalog es un portal web oficial donde puedes encontrar las actualizaciones de seguridad publicadas para los sistemas operativos Windows.

Utiliza soluciones de seguridad

En un sistema operativo como Windows, el más usado y por ello el más atacado, es probable que hasta el usuario más prudente en el uso de su equipo tenga que lidiar con algún tipo de infección. Y de ahí la necesidad de usar algún tipo de software que nos ayude en la tarea. Para Windows (también para iOS y Android) Microsoft ofrece Windows Defender como solución de seguridad nativa. Aunque fue lanzada en su origen como una solución básica, con los años ha mejorado enormemente en capacidad de detección y resolución y hoy es suficiente como protección básica para la mayoría de consumidores.

Por supuesto, puedes usar soluciones de proveedores especializados que ofrecen un buen número de soluciones de seguridad, muchos de ellos gratuitos. Un usuario avanzado o profesional debería valorar el uso de una suite de seguridad comercial integral que incluya herramientas adicionales como un firewall y otras especializadas contra ataques de Ransomware, Phishing, adware o spyware.

- **Gestiona bien las contraseñas**: Otra de las reglas de oro para mejorar la seguridad en Internet (además de usar técnicas avanzadas de identificación biométrica si el dispositivo que uses lo permite) es tener una contraseña fuerte y distinta para cada sitio web.

Las contraseñas fuertes previenen los ataques de fuerza bruta y el uso de una contraseña diferente para cada cuenta evita tener todas ellas comprometidas a la vez cuando se produce una violación de datos.

Debes seguir una serie de reglas para su creación y valorar el uso de gestores de contraseñas.

- **Utiliza una llave de seguridad hardware para cuentas vitales:** Para cuentas vitales, especialmente en entornos profesionales y empresariales, conviene hacer un esfuerzo adicional para protegerlas usando un mecanismo de seguridad por hardware. Generalmente es un dispositivo en formato pendrive que se conecta a un puerto USB y contiene un motor de cifrado de alta seguridad. Todo el proceso se realiza dentro del hardware aumentando enormemente la

seguridad general frente a las soluciones por software.

- **Evita las redes inalámbricas gratuitas**: Los puntos de acceso gratuitos se han extendido por múltiples zonas en poblaciones, zonas de restauración, aeropuertos, estaciones de tren o metro, hoteles y en todo tipo de negocios. Darkhotel, la Amenaza Persistente Avanzada (APT) descubierta por Kaspersky Lab, confirmó la inseguridad intrínseca de las redes inalámbricas públicas.

Llevaría activa desde 2007 y se habría dedicada a obtener información privilegiada de ejecutivos y empleados de alto nivel alojados en hoteles de alta categoría. Investigadores de seguridad han demostrado que este tipo de redes son fácilmente hackeables por lo que únicamente deberíamos utilizarlas para navegación ocasional y sin revelar nuestros datos personales nunca.

Con información de Ultimas Noticias