Publicado en Ciudad de México el 10/10/2018

# [La guía esencial de Avast para la seguridad de Mac](http://www.notasdeprensa.es)

## Históricamente, los usuarios de Mac han manejado registros de seguridad excepcionales durante décadas, pero todo está cambiando, y los hackers están aprendiendo a sortear los protocolos de seguridad de Mac

 Renovar un equipo de cómputo no es tarea fácil, más allá de las marcas y modelos, los usuarios se enfrentan a elegir entre el sistema operativo Windows o Mac. Windows es el sistema más utilizado en el mundo, porque es ofrecido por una gran variedad de compañías y también el más susceptible a sufrir ataques, como el ataque de ransomware masivo WannaCry que se propagó en Windows e infectó más de 230,000 equipos el año pasado. Por su parte, las Mac son máquinas reconocidas por sus diseños elegantes, su sistema operativo intuitivo, sus aplicaciones que marcan tendencia, pero, ¿qué tan cierto es que no hay virus que infecten las Mac? ¿Es realmente necesario el software antivirus para una Mac? Históricamente, los usuarios de Mac han manejado registros de seguridad excepcionales durante décadas, y esto es por dos razones. Una es que las Mac están construidas con fuertes características de protección y muy pocas vulnerabilidades explotables, y la otra es que la mayor parte del mundo posee computadoras, de modo que es ahí donde los ciberdelincuentes han enfocado sus esfuerzos para sacar ventaja. Pero todo está cambiando, y los hackers están aprendiendo a sortear los protocolos de seguridad de Mac. Con el KeRanger de 2016, el primer ransomware troyano para Mac OSX, y el Patcher de 2017, un ransomware para Mac que se extendió a través de BitTorrent, se ha visto que las Mac no son completamente invulnerables. Su seguridad es sólida desde el primer momento, es cierto, pero hay varias configuraciones de seguridad adicionales que refuerzan su protección si se las configura. Además, existen algo más que simples ataques de malware en Mac que deberían tomarse en cuenta: los ciberdelincuentes siempre están creando sitios web falsos, correos electrónicos de suplantación de identidad (phishing) y más, todo con la intención de tomar el control de los dispositivos de los usuarios. Entonces, ¿qué se puede hacer? Instalar un antivirus, como Avast Security para Mac es el primer paso. Además de poner en práctica los siguientes 4 consejos para mejorar las defensas de seguridad. Consejo Mac # 1: Revisar la configuración de `Seguridad y privacidad´ de MacOS El paso más importante es establecer una contraseña para inicio de sesión. Avast recomienda utilizar contraseñas seguras y dejar fuera las tradicionales “12345” o “contraseña”. Posteriomente, se recomienda activar FireVault ya que de esa manera, su Mac cifrará los datos en su disco duro. Asimismo, encender Firewall para proteger la red al bloquear el tráfico entrante no deseado, con lo que cualquier red externa que intente hacer ping no recibirá respuesta. Consejo de Mac # 2 - Saber lo que se está compartiendo En Preferencias del sistema al hacer clic en “Compartir”, se puede revisar la lista y asegurarse de que solo se está compartiendo lo que absolutamente se necesita compartir. Si no es esencial, es preferible no hacerlo. Consejo de Mac # 3 - Siempre actualizar, siempre copia de seguridad Cuando se emiten actualizaciones, están destinadas a mejorar el sistema, generalmente en forma de seguridad. Al actualizar los parches, se fortalece la seguridad y mejora el rendimiento. Algunos temen que si actualizan su sistema, perderán algo de información o serán confundidos por las nuevas reglas y herramientas. Avast buscar desmentir este temor infundado entre los usuarios finales y hacerles comprender que una actualización del sistema es su aliada. Consejo de Mac # 4 - Instalar seguridad cibernética extra Los protocolos de seguridad de Apple son excelentes, pero para estar un paso adelante del sofisticado delito cibernético los usuarios necesitan blindarse con un software adicional de seguridad y privacidad, como: • Antivirus. Instalar un potente antivirus para Mac es un excelente paso para defender la Mac. Avast Security para Mac es gratuito y protege contra malware, sitios web maliciosos y conexiones Wi-Fi vulnerables. Para el más alto nivel de seguridad, obtenga protección contra: Ransomware y transparencia a cualquier intruso wifi adquiriendo la versión Mac Security Pro. • Red privada virtual (VPN). Para cifrar la conexión a Internet y mantener la privacidad en línea, Avast recomienda utilizar una VPN como Avast SecureLine VPN. Si bien los ciberdelincuentes se enfocaban predominantemente en las PC en el pasado, cada vez más están desarrollando malware para las Mac. Avast exhorta a los usuarios a dejar de creer que las Mac son ajenas a los ataques, en el mundo digital, no hay precauciones de más.

**Datos de contacto:**

Marketing Q S

Agencia de Relaciones Públicas

+ 52 55 5615

Nota de prensa publicada en: [https://www.mexicopress.com.mx/la-guia-esencial-de-avast-para-la-seguridad-de](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Hardware Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)