Publicado en Ciudad de México el 27/09/2018

# [Avast comparte las reglas de oro para evitar ser descubierto por los hackers](http://www.notasdeprensa.es)

## Actualmente, cualquier persona famosa puede ser un objetivo de los hackers, ya que ellos siempre están buscando maneras de beneficiarse a través de otros

 En el pasado, se ha visto un incremento en ataques de hackers dirigidos a personas famosas, desde artistas, deportistas y hasta políticos. Actualmente, cualquier persona famosa puede ser un objetivo de los hackers, ya que ellos siempre están buscando maneras de beneficiarse a través de otros. Existen casos famosos como el de Justin Bieber, donde se filtró su foto desnuda en la cuenta más seguida de Instagram, la de Selena Gómez. Afortunadamente, la escandalosa imagen fue eliminada rápidamente, la cuenta de Selena se bloqueó y el acceso a Gómez fue luego devuelto. Sony Pictures protagonizó el escándalo del año cuando hackers filtraron documentos y correos electrónicos de los principales productores de Sony Pictures Entertainment, con lo que se afectó la reputación de la compañía de entretenimiento y de muchos de sus ejecutivos. Siendo el más sonado aquel que involucró a los principales productores de la compañía Scott Rudin y Amy Pascal, quienes calificaron a Angelina Jolie como and #39;chica mediocre consentida and #39;. Posteriormente, los productores se disculparon por los insultos contra Jolie y otras estrellas. Sin embargo, el mal ya estaba hecho. Dirigentes políticos también han sido víctimas. Basta recordar el hackeo a la cuenta de Twitter del ex primer ministro de Rusia, Dmitry Medvedev. Una mañana, la cuenta del político difundió mensajes en los cuales Medvedev admitía que estaba avergonzado de las acciones del gobierno, por lo que se vería obligado a renunciar. Afortunadamente para el primer ministro, retomó el control de la cuenta. El exjugador de fútbol de Inglaterra David Beckham se negó a pagarles a los hackers un rescate de 1 millón de euros por su información y recurrió a la policía. En respuesta a esto, los ciberdelincuentes enfadados hicieron circular por la red la correspondencia de Beckham. En ella manifestaba estar muy interesado en obtener el título de Caballero y, cuando se le fue negado, habló groseramente de los miembros del comité Whitehall. Cristian Gallardo, Gerente Regional de Avast en América Latina, está de acuerdo con las acciones tomadas por Beckham para afrontar el incidente. En ningún caso se recomienda pagar rescate. Primero, no hay garantía de que los datos no se filtren y, en segundo lugar, la recompensa financiera solo alentará a los hackers a realizar más intrusiones.​ A continuación, Avast, líder global en productos de seguridad digital para consumidores y empresas, comparte las reglas de oro que los usuarios deben cumplir para evitar ser hackeados: Crear contraseñas seguras. No se debe usar la misma contraseña para todas las cuentas. Tras tener una contraseña, un atacante puede acceder a todas, a la vez. Se recomienda utilizar contraseñas complejas con números, símbolos y letras mayúsculas. Existen aplicaciones para generar y guardar contraseñas de manera segura. El programa creará contraseñas seguras para cada cuenta y le permitirá cambiarlas fácilmente. El usuario simplemente deberá recordar la contraseña para iniciar sesión en este programa. Utilizar la autenticación de dos factores. Por razones de seguridad, muchas empresas han introducido una función de autenticación de dos factores. Al ingresar un nombre de usuario y contraseña, se enviará una contraseña de un solo uso al teléfono móvil o dirección de correo electrónico del usuario, misma que debe ingresar para iniciar sesión en su cuenta. Esta función le permite crear un segundo nivel de protección contra hackers. No abrir enlaces ni archivos sospechosos. A menudo, los usuarios mismos proporcionan acceso a sus dispositivos, debido a que visitan enlaces que no son de confianza y abren archivos sospechosos. Cuando esto sucede, se instala un programa malicioso en el dispositivo móvil o PC. Por ejemplo, los ciberdelincuentes a menudo esconden iconos de programas o los disfrazan en el dispositivo para crear dificultades al eliminar el malware. Los objetivos de estos programas son diferentes: pueden esperar mucho tiempo, hasta que, por ejemplo, vaya a la aplicación de banca móvil para robar datos para ingresar. De la misma manera, puede robar inicios de sesión y contraseñas a cualquier cuenta. Además, los hackers pueden acceder a casi cualquier información en el teléfono inteligente. Descargar programas de fuentes confiables. Instalar software de fuentes no confiables puede llevar a muchas consecuencias desagradables. Con dicho software malicioso, puede robar datos personales, así como causar daños graves al dispositivo o a la computadora en su conjunto. Elegir tiendas de aplicaciones confiables, como App Store y Google Play. Cambiar el nombre de usuario y la contraseña del router. A menudo, los usuarios dejan su nombre de usuario y contraseña de forma predeterminada, es decir, la que viene por defecto en el router. Esto es un gran error, ya que las contraseñas estándar se pueden encontrar fácilmente en Internet. "El router es frecuentemente mal comprendido o subestimado, pero es indiscutiblemente el dispositivo más importante, pues actúa como puerta de entrada a internet. Al conectar diferentes dispositivos y al permitirles compartir datos entre sí, mientras administra el tráfico web entrante y saliente, se convierte en el blanco natural de agentes maliciosos, los cuales están intentando hacerse con información sensible, como los datos para el ingreso a cuentas bancarias, y sustrayendo información de los dispositivos emparejados con ellos, como los dispositivos conectados a la Internet de las Cosas. Como medida mínima de protección, las personas deberían cambiar los usuarios y contraseñas que traen por defecto sus enrutadores, tan pronto como los instalan y proactivamente verificar las actualizaciones del firmware". Tener cuidado al conectarse a Wi-Fi públicas. Una de las maneras más comunes por las cuales los hackers obtienen la información sensible de los usuarios es a través de puntos de acceso gratuitos a Wi-Fi. Es muy simple: cuando un usuario se conecta a Wi-Fi, un hacker accede a su dispositivo y puede robar prácticamente cualquier información. Para evitar lo anterior, se recomienda utilizar servicios de VPN confiables que oculten las actividades en internet del ojo cibernético de los intrusos.

**Datos de contacto:**

Marketing Q S

Agencia de Relaciones Públicas

+ 52 55 5615

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-comparte-las-reglas-de-oro-para-evitar\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional E-Commerce Ciberseguridad Dispositivos móviles Ciudad de México



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