



McAfee revela unos sencillos consejos para mantener seguros nuestros dispositivos conectados a internet, especialmente en Navidad

Madrid, 15 de Diciembre de 2011 – Desde el último tablet hasta el portátil de moda, los dispositivos electrónicos se encuentran en los primeros puestos de la carta que escribimos a los Reyes Magos. Aquellos que reciban este tipo de regalos tecnológicos, inmediatamente guardarán sus datos personales, información de sus contactos y fotos, para disfrutar de su nuevo dispositivo.

McAfee nos advierte de que no seamos tan rápidos, porque cuando los nuevos dispositivos están completamente desprotegidos, bastan unos clics para que nuestra información personal sea robada o nuestro dispositivo infectado de malware.

“Para estar protegidos es importante que los consumidores implementen seguridad en sus nuevos dispositivos desde el mismo momento en el que los compran”, afirma Gary Davis, director de marketing de producto de consumo de McAfee. “La buena noticia es que ahora es más sencillo y eficaz hacerlo, ya que los consumidores pueden comprar una solución para proteger todos sus dispositivos y gestionarla fácilmente desde una única interfaz. Esto es el incentivo necesario para que los usuarios protejan todos sus dispositivos desde el principio y disfrutar de ellos sin preocupaciones.”

McAfee anima a los consumidores a que pongan en práctica algunas precauciones para mantener seguros sus dispositivos:

1. Protege tus datos almacenados en los dispositivos móviles. En una [reciente encuesta realizada por McAfee](#), el 60% de los usuarios tienen, al menos 3 dispositivos y el 25% de ellos cuenta con 5. De esta misma encuesta se desprende que los usuarios valoran en 37.000 dólares los activos digitales almacenados en ellos. Considera la posibilidad de utilizar un producto que ofrezca copia de seguridad de datos y funciones de restaurar, así como seguridad avanzada que permita localizar el dispositivo, bloquearlo por control remoto y eliminar los datos, en caso de que sea perdido o robado. Esto es importante porque un 30% de los usuarios no realiza copias de seguridad de sus archivos, y lo que es peor, cada tres segundos falla un disco duro.
2. Si tienes un producto de Apple, toma las mismas precauciones que con PC, ya que su popularidad les ha hecho ser el blanco de las amenazas. Y es que, según los Laboratorios McAfee Labs, a finales de 2010, había 5.000 piezas de malware dirigidas contra Mac y están aumentando a razón de un 10% al mes. Como medida proactiva, instala un software de seguridad que haya sido desarrollado por Mac, como por ejemplo el nuevo servicio iCloud.

3. Si tienes un nuevo PC o un netbook, asegúrate de que cuentas con un software de seguridad que incluye como mínimo antivirus con cloud computing, firewall bidireccional, antispam y funciones de búsqueda segura. Los niveles adicionales de protección deben incluir antispam, control parental, protección de red wireless, protección de robo de identidad que encripte documentos con información confidencial. Un antivirus no es suficiente, ya que se encuentran 8.900 nuevos sitios web diariamente y el malware tuvo un coste, solo en Estados Unidos, de 2.300 millones de dólares el año pasado.
4. El software de seguridad gratuito puede dejarte desprotegido, ya que proporciona protección básica, que con frecuencia, se utiliza como gancho para que el usuario compre más productos. Instala un software de seguridad que proporcione protección actualizada utilizando cloud computing, que te ayude a estar protegido.
5. Realiza búsquedas y compras online de forma segura. Para que no accedas a sitios web peligrosos, utiliza McAfee SiteAdvisor, incluido en todas las suites de seguridad de consumo, que indica qué sitios web son seguros y cuáles entrañan riesgo. Además, cuando hagas compras en la red, busca la marca de confianza McAfee SECURE™, que indica que el sitio web ha superado rigurosos test para 10.000 vulnerabilidades conocidas.
6. Pon especial atención en los antivirus falsos o “scareware” que pretenden hacerte creer que el PC puede estar infectado para que compres antivirus falsos y así robar tu información personal y financiera, generalmente a través de ventanas emergentes. Debes tener en cuenta los siguientes datos:
 - El scareware ha crecido un 600% de 2008 a 2010 y se estima que tiene un millón de víctimas al día.
 - En 2011, por primera vez un antivirus falso para Mac se ha convertido en una herramienta para los cibercriminales.
 - No adquieras software de seguridad a través de ventanas emergentes.
7. Educa a tu familia y pon especial atención en las actividades de los niños en internet. Mantén el PC en un área común y aclárales qué tipo de información es apropiada para compartir en la red y cuál no, como la dirección física, el número de teléfono y cualquier otro tipo de información privada.
 - Si tienes hijos pequeños, limita su acceso a la red y el contenido que pueden ver. Utiliza una herramienta de filtrado web que protege a los niños de acceder a contenido inapropiado.
 - No asumas que tus hijos no saben desconectar el control parental
8. Si tú o tus hijos tienen un nuevo juego (Nintendo Wii o 3DS, PlayStation 3, Xbox 360), recuerda que estos dispositivos están conectados a internet y, por tanto, son vulnerables a las mismas amenazas que los PCs. Haz copias de seguridad de los juegos y aprovecha el control parental que incluyen para proteger a los niños de juegos violentos o limitar cuándo deben ser utilizados estos dispositivos.

- Algunos juegos de múltiples jugadores permiten jugar en internet con personas que no conocemos, así que considera el uso de una herramienta de monitoreo de actividades. Conecta el dispositivo solo a una red Wi-Fi segura.
 - No guardes información personal en tu dispositivo.
9. Si tienes un dispositivo USB o un disco duro portátil, utiliza las tecnologías que protegen tu información. Considera la posibilidad de utilizar un USB encriptado para que no sea posible leer la información que contiene si es perdido o robado.
10. Si tienes un nuevo smartphone o tablet, debes ser consciente de que las amenazas dirigidas a dispositivos móviles están creciendo. De hecho, los ataques contra Android han aumentado un 37% en el tercer trimestre del año, comparado con el trimestre anterior. Por tanto, vigila que las aplicaciones que descargues sean de una tienda oficial. Considera la posibilidad de [utilizar protección contra amenazas de malware a dispositivos móviles](#). Para los usuarios que tengan muchos dispositivos, [McAfee® All Access](#) es una solución sencilla para proteger una amplia gama de dispositivos conectados a internet.

McAfee

McAfee, empresa subsidiaria propiedad de Intel Corporation (NASDAQ:INTC), es líder en tecnología de seguridad. McAfee tiene el firme compromiso de afrontar los más importantes retos de seguridad. La compañía proporciona servicios y soluciones probados y proactivos que ayudan a proteger redes, dispositivos móviles y sistemas en todo el mundo, permitiendo a los usuarios conectarse a Internet, navegar por la Web y realizar compras online de forma más segura. Gracias a la tecnología Global Threat Intelligence (Inteligencia Global de Amenazas), McAfee proporciona protección en tiempo real mediante sus soluciones de seguridad, permitiendo a las empresas, usuarios particulares, organismos públicos y proveedores de servicios cumplir con la normativa, proteger datos, prevenir interrupciones, identificar vulnerabilidades y controlar cualquier tipo de amenaza que pueda poner en peligro su seguridad. En McAfee enfocamos todos nuestros esfuerzos en la búsqueda constante de nuevas soluciones y servicios que garanticen la total seguridad de nuestros clientes. <http://www.mcafee.com/es>

Nota: McAfee y App Alert son marcas comerciales de McAfee, Inc. y/o de sus empresas filiales en Estados Unidos y otros países. Otras marcas pueden ser reclamadas como propiedad de otros. © 2011 McAfee, Inc. Reservados todos los derechos.

Para más información:

<p>McAfee Eva Martín Marketing Manager eva_martin@mcafee.com Marie Luszcz Marketing Assistant Marie_Luszcz@McAfee.com Tel: +34 91 347 85 00</p>	<p>Porter Novelli Palmira Muñoz palmira.munoz@porternovelli.es Virginia Cabeza virginia.cabeza@porternovelli.es Tel: +34 91 702 73 00</p>
--	--