Seguridad en la Red

Información y prevención

Es necesario partir de la siguiente premisa: "La seguridad total no existe". A resultas de esta máxima, la única herramienta eficaz de la que disponemos es la información y la prevención. Por ello, aquí os dejamos unos consejos básicos necesarios para desenvolverse en la Red de Redes.

Diego **Guerrero**

Lo primero y fundamental es tener nuestro Mac actualizado, es decir, tener instaladas las últimas versiones del sistema operativo, navegador web y actualizaciones de seguridad, así como una conexión inalámbrica protegida por WPA o WPA2**(1)**. También es muy recomendable desactivar todas las opciones de compartir servicios en el panel de preferencias Compartir, no abrir puertos del router y, en caso de trabajar con archivos cuyo origen y destino sea un ordenador Windows, podemos emplear un antivirus actualizado para detectar y eliminar posibles virus. Aunque nuestro Mac sea inmune a las infecciones por virus, es un buen detalle para quienes no tienen la suerte de trabajar con OS X. Además, existen algunos virus-macro que afectan al entorno de trabajo de Microsoft Office, incluso en versión Mac. Estas medidas solucionan gran parte de las vulnerabilidades de nuestros ordenadores.

Comercio electrónico y compras en línea

Antes de realizar cualquier compra en línea, asegúrese de que la empresa vendedora dispone en su página web de una pasarela de pagos segura. Las direcciones web donde se introduzcan datos personales y de pago deben comenzar por "https://" y debe aparecer el dibujo de un candado en su navegador.

Consejo: ***Haciendo clic con el cursor sobre el icono del candado podrá ver y comprobar el certificado de seguridad de la página web.***

No acepte pagar en ningún caso por ningún tipo de servicio de envío de dinero, pues este no es nunca el método de pago empleado por una empresa seria.

Truco: ***Haga una búsqueda en Internet con el nombre de la tienda, obtendrá muchos resultados. Si la mayoría son negativos, ¡desconfíe!***

Si va a realizar la compra a un particular, con el que ha contactado por medio de un foro o una página de compra-venta, tenga en cuenta que es importante saber con quién se trata. Reúna todos los datos posibles. Si va a pagar por transferencia bancaria solicite a su banco un recibo, y no olvide poner el concepto exacto y el destinatario.

Desconfíe de los anuncios de venta donde se ofrecen productos de alto valor a un precio muy por debajo del mercado. Si se le solicita que ingrese o envíe una cantidad de dinero como señal, ¡no lo haga!

Si va a pagar contra reembolso, debe saber que algunas agencias de mensajería permiten la apertura del paquete antes del pago, en esto deben estar de acuerdo comprador y vendedor, pues es un servicio extra y como tal hay que solicitarlo.

Procure guardar copias de todo: anuncio de venta, mensajes privados, mensajes de correo, direcciones de correo y de la web donde se anunciaba.

Un método muy recomendable, y que nos puede ahorrar más de un susto, consiste en disponer de una cuenta bancaria y una tarjeta de débito asociada a esta, que utilizaremos exclusivamente para nuestras transacciones en Internet. De esta manera, en dicha cuenta sólo dispondremos del efectivo

suficiente para estas operaciones, y aunque nuestros datos cayeran en malas manos no se podría obtener ningún beneficio.

Phishing y derivados

Debe tener siempre presente que ni su banco, ni su ISP, ni cualquier otro servicio, le pedirán nunca por correo que, por motivos de seguridad, administración o cualquier otro, introduzca sus datos personales.

Siempre que desee acceder a cualquier servicio bancario en línea, abra una ventana nueva de su navegador y teclee personalmente la dirección del mismo. Jamás lo haga mediante enlaces o hipervínculos que reciba por correo o vea en cualquier otra web.

Asegúrese de encontrarse en un servidor seguro y que la dirección que vea en la barra de direcciones sea la que corresponde con el sitio oficial de su entidad. Recuerde que las direcciones de servidores seguros han de comenzar por "https://"

A tener en cuenta:

✔ No introduzca ningún dato en los formularios de los que desconozca su origen.

✔ No haga clic con su ratón en los enlaces bancarios recibidos por correo.

✔ Asegúrese de estar en un servidor seguro antes de realizar cualquier operación.

Correo electrónico, estafa y fraude.

Desconfíe de cualquier mensaje que reciba de remitente desconocido. Por muy sugerente que le resulte el asunto, lo mejor que puede hacer es borrarlo directamente.

Tenga cuidado con las ofertas de trabajo que reciba por correo, principalmente de aquellas que ofrecen condiciones muy ventajosas. Habitualmente se le ofrecerá que gestione a través de sus cuentas ciertas cantidades de dinero, por las que usted se quedarán un porcentaje. Esta es una versión moderna del timo de "las cartas nigerianas", y con ello usted esta blanqueando dinero procedente de actividades ilícitas y, por lo tanto, cometiendo un delito.

Procure no caer en la tentación de reenviar los mensajes en cadena (conocidos como *hoax*) pues solo conseguirá perjudicar y congestionar los servidores de correo, así como facilitar una gran base de datos de cuentas de correo al autor, que habitualmente son vendidas y usadas para el envío de mensajes de publicidad no deseados (el famoso *spam*)**(2)**.

Consejos generales

✔ Mantenga su sistema operativo actualizado.

✔ Emplee un cortafuegos.

✔ Haga copias de seguridad de sus datos periódicamente.

✔ Utilice contraseñas avanzadas, compuestas de números, letras y símbolos. Cámbielas periódicamente.

✔ Borre el correo basura (*spam*) sin leerlo.

Nunca proporcione datos personales o bancarios en páginas web no seguras o formularios recibidos por correo electrónico.

✔ En redes Wi-Fi públicas, evite acceder a cualquier servicio que requiera nombre y contraseña, como banca electrónica, redes sociales, correo...

Esta es una pequeña guía orientativa para poder protegerse de forma más efectiva en la Red. No obstante, la mejor herramienta es el propio sentido común y la experiencia. ¡Úselos! ■

Diego Guerrero es autor del libro: "Fraude en la Red", de la editorial Ra-Ma.

Nota 1: Ayudará a protegernos de intrusos que se aprovechen de nuestra red, pero además nos aseguraremos de que no vean el tráfico del resto de nodos. Para configurar la protección de la red inalámbrica disponemos de los sistemas de cifrado. Los más seguros son WPA y WPA2, que están soportados por estaciones base y tarjetas Airport actuales, a los que accederemos desde la administración de nuestro Airport. Como cualquier clave, mejor cuanto más larga y aleatoria sea.

Nota 2: Activar filtros anti-spam. Para activar el filtro de correo no deseado, especificaremos en preferencia de Mail >> "Correo no deseado" las acciones que deben ejecutarse cuando nos llegue correo de este tipo. También es una práctica recomendada desactivar la carga automática de imágenes remotas (podremos cargarlas manualmente al recibir mensajes) en las preferencias de Mail >>Visualización, desmarcando la casilla "Mostrar imágenes remotas en los mensajes HTML". Consulta la ayuda de Mail, o tu gestor de correo, para más información.

a saber

Enlaces de interés

- ***http://www.macuarium.com/cms/index.php?option=com_remository&Itemid=169&func=startdown&id=335***
- ***http://www.macuarium.com/actual/especiales/2004/10/28_opener.shtml***
- ***http://www.macuarium.com/foro/index.php?showtopic=147600***