CONSEJOS DE SEGURIDAD
MCAFEE MULTIDISPOSITIVOS DE ETB

Además de instalar nuestros productos, le recomendamos tomar estas simples y prácticas precauciones para reducir su nivel de exposición y proteger su sistema.

1. **No abra ningún archivo adjunto al correo electrónico procedente de un remitente desconocido, sospechoso o poco fiable:** Si no conoce al remitente, no abra ni descargue ni ejecute ningún archivo ni datos adjuntos al correo electrónico.

2. **No abra ningún archivo adjunto al correo electrónico a menos que sepa lo que es, aunque parezca que procede de un amigo o de alguien que conoce:** Algunos virus se auto reproducen y se propagan a través del correo electrónico. Procure ser cuidadoso y confirme que el archivo adjunto procede de una fuente de confianza antes de abrirlo.

3. **No abra ningún archivo adjunto al correo electrónico si la línea de Asunto es dudosa**: Si cree que el archivo adjunto es importante, guárdelo siempre en su disco duro antes de abrirlo.

4. **Borre los correos en cadena y otro tipo de spam de su buzón de entrada:** Es conveniente no reenviar ni responder este tipo de mensajes. Los correos electrónicos no solicitados e intrusos obstruyen la red, pueden tener contenido molesto u ofensivo y pueden generar riesgos para la seguridad y la privacidad.

5. **Sea precavido cuando descargue archivos desde Internet:** Asegúrese de que el sitio Web es legítimo y de confianza. Verifique que un programa antivirus haya analizado los archivos en el sitio de descarga. Si tiene alguna duda, no descargue el archivo. Si descarga programas de software de Internet, tenga especial cuidado con los programas gratuitos, que con frecuencia contienen programas publicitarios u otro contenido posiblemente no deseado. Siempre lea las políticas de privacidad y los acuerdos de licencia del usuario final (EULA) de los programas de software que instale, sin importar su origen. Tenga especial precaución con los protectores de pantalla, juegos, complementos del explorador, clientes punto a punto (P2P) y cualquier descarga que afirme ser "crackeada" o una versión gratuita de aplicaciones costosas como Adobe® PhotoShop® o Microsoft® Office. Parece muy bueno para ser verdad y probablemente no lo sea.

6. **Evite totalmente descargas de fuentes no web:** Las posibilidades de descargar programas de software infectados de grupos Usenet, canales IRC, clientes de mensajería instantánea o programas punto a punto son muy altas. Los vínculos a sitios Web vistos en IRC y la mensajería instantánea suelen llevar con frecuencia a descargas infectadas. Evite obtener programas de software de estas fuentes.

7. **Actualice su software antivirus con frecuencia:** La cantidad de amenazas es cada vez mayor y están en constante evolución. Cada mes se descubren cientos de virus. A fin de asegurar que usted se encuentre protegido contra las amenazas más recientes, actualice su software antivirus con frecuencia. Esto implica descargar los archivos de firmas antivirus más recientes y la versión más actualizada del motor de exploración.

8. **Haga copias de seguridad de sus archivos con frecuencia:** Si un virus infecta los archivos, por lo menos podrá sustituirlos por los de la copia de seguridad. Es conveniente almacenar sus archivos de respaldo (en CD o unidades "flash") en otra ubicación física segura lejos de su computadora.

9. **Actualice su sistema operativo, su navegador Web y su programa de correo electrónico con regularidad:** Por ejemplo, Microsoft® ofrece actualizaciones de seguridad para Microsoft Windows y Microsoft Explorer en http://www.microsoft.com/security.

10. **Una actitud vigilante es la mejor defensa contra el fraude electrónico:** El término "phishing" hace referencia a fraudes que intentan obtener información confidencial, como números de tarjetas de crédito, datos personales de identidad y contraseñas, mediante el envío de mensajes de correo electrónico que parecen proceder de empresas reales o personas de confianza. Si recibe un mensaje por correo electrónico que le avisa del cierre de una de sus cuentas, le pide que confirme una orden o le indica que verifique información de facturación, no conteste al mensaje ni haga clic en ningún vínculo. Si desea averiguar si el mensaje es legítimo, llame por teléfono o escriba directamente a la empresa o la persona.

11. **No abra mensajes ni haga clic en enlaces provenientes de usuarios desconocidos en su programa de mensajería instantánea:** La mensajería instantánea puede ser un vehículo para transmitir virus y otros códigos maliciosos y constituye otra forma para emitir mensajes de fraude electrónico.

12. **Use un firewall personal:** Un firewall de hardware que resida entre su enrutador DSL o módem lo protegerá de ataques entrantes. Es un requisito fundamental para conexiones de banda ancha. Un firewall de software se ejecuta en su PC y puede protegerlo contra ataques entrantes y salientes.

13. **Revise sus cuentas e informes de crédito en forma regular:** Los ladrones de identidad pueden comenzar a usar su información personal para abrir cuentas, comprar bienes y hacer de su vida un infierno en minutos luego de adquirir dicha información. Revise sus estados de cuenta e informes de tarjetas de crédito con frecuencia. De esta forma, podrá descubrir si su información personal se ha visto comprometida y así notificar a los bancos y entidades crediticias de inmediato para que cierren sus cuentas.