

RECOMENDACIONES DE SEGURIDAD TRAS EL PUENTE DE OCTUBRE

Cuando vuelva del puente tenga cuidado con el e-correo no solicitado: podría ser víctima de un fraude on-line

El notable incremento de ataques informáticos durante períodos vacacionales, semana santa, verano y puentes, normalmente ocultos tras los correos no deseados o no solicitados. [Correos falsos que simulan proceder de entidades bancarias \(denominados phishing \) y ofertas laborales sospechosas \(llamadas scam \)](#), son algunos de los métodos utilizados por redes de ciberdelincuencia que han multiplicado notablemente su actividad durante el año 2007, obliga a los internautas a tomar algunas precauciones para la seguridad de sus Pcs.

Consejos a tener en cuenta cuando se acceda a los servicios de correo y mensajería a la vuelta de las vacaciones:

MEDIDAS GENÉRICAS

1.- Mantenimiento. El final de periodo vacacional es un momento ideal para realizar tareas de mantenimiento que serán muy saludables para el rendimiento de su ordenador:

- Borrar aplicaciones, juegos, documentos, carpetas, etc., que puedan haber quedado obsoletos.
- Usar la herramienta del sistema operativo destinada a liberar espacio del disco duro.
- Defragmentar los discos para reagrupar información y mejorar la velocidad de acceso.
- Mantener el sistema operativo y software de aplicación actualizado con los últimos parches.
- Hacer copias de seguridad y discos de recuperación. Utilice para ello CD, DVD o discos duros externos.

2.- Software legal: sólo el software adquirido por cauces legítimos cuenta con garantía comercial y legal, mientras que las copias piratas presentan grandes riesgos ante problemas de seguridad, carecen de garantías y resulta imposible realizar reclamaciones.

MEDIDAS BÁSICAS DE SEGURIDAD

1.- Antivirus: antes de conectar su ordenador a la red, compruebe que tiene instalado un antivirus de escritorio o una aplicación similar suministrada por su proveedor de servicios. Actualice, si es necesario, éstas aplicaciones antes de abrir su correo electrónico o navegar por la red.

2.- Cortafuegos: un cortafuegos o "firewall" es un software destinado a garantizar la seguridad en sus comunicaciones vía Internet al bloquear las entradas sin autorización a su ordenador y restringir la salida de información. Es imprescindible utilizar este tipo de software si dispone de conexión ADSL, y muy aconsejable en el resto de casos. Verifique su estado y configuración a la vuelta de vacaciones.

3.- Correo electrónico: desconfíe de aquellos correos que le llegan en idiomas que desconoce, que proceden de direcciones desconocidas, que incluyen videos y fotos asegurando que deben ser vistos,

o que ofrecen productos mágicos, vacaciones gratuitas, trabajos altamente remunerados, dinero fácil o le premian a actualizar su información bancaria.

4.- Usuarios y Contraseñas: otorgue a los usuarios privilegios acordes al uso que vayan a hacer del ordenador y mantenga una política de contraseñas fuerte según se describe en <http://www.alerta-antivirus.es>

5.- Chat-mensajería instantánea: las principales amenazas son los mensajes con invitaciones a ver sitios web que en la mayoría de los casos albergan programas para la descarga de códigos maliciosos. Otras amenazas llegan a través de fotos y vídeos. En general habrá que observar las máximas precauciones a la hora de conversar y agregar contactos de desconocidos, especialmente los internautas más pequeños de la casa.

6.- P2P. Compartir ficheros: P2P es una aplicación confiable, no necesariamente sus usuarios. En efecto, los contenidos aportados por algunos usuarios malintencionados son los que provocan las infecciones y la desconfianza en este sistema de intercambio de información;

- No comparta software ilegal

- Antes de abrir cualquier archivo descargado, analícelo con su antivirus actualizado y/o alguno en línea.

7.- Seguridad en móviles: si su teléfono móvil está equipado con conexión bluetooth y no va a usar esta funcionalidad, mantenga este tipo de conexión desactivada o en su defecto actívela únicamente durante el tiempo que vaya a utilizarla. Tenga cuidado con las descargas en su teléfono móvil, al igual que en un PC, podrían instalarse marcadores de teléfono automáticos (dialers), archivos que permitan el acceso no autorizado a información de su dispositivo móvil (troyanos), etc.

8.- Phishing por teléfono: en algunos países están apareciendo llamadas simulando proceder de entidades financieras. Estas llamadas solicitan datos de sus cuentas bancarias que les permiten tener acceso a su dinero. Esta tendencia puede llegar a nuestro país, por tanto desconfíe de cualquiera que le pida el número de cuenta, contraseñas, etc., por teléfono.

Otra modalidad de este tipo de fraude es la recepción de mensajes al móvil (sms) o correo electrónico invitando a llamar a números de teléfono gratuitos por ejemplo para reactivar su cuenta de correo o cancelar una compra que le han cargado a su cuenta bancaria. No llame a estos teléfonos proporcionados y verifique esta información con su banco o compañía a través de su contacto habitual.

9. - La información es la mejor vacuna

Además de estas recomendaciones existe una regla de oro para protegerse tanto de virus informáticos como de cualquier posible peligro de la red: esté atento a los medios de comunicación, en general, que le informarán de los incidentes más comunes en la red española, y visite regularmente las páginas de información sobre seguridad informática.

Fecha artículo: 2007-10-14 07:29:33 - url artículo: <http://www.internautas.org/html/4326.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org