Taller de seguridad digital con Juan Carlos Solís

Llevado a cabo en Hotel Benidorm, Distrito Federal, México, los días 24 y 25 de agosto de 2013

Relatoría de Periodistas de a Pie

Las computadoras e internet son las herramientas de trabajo por excelencia en nuestros tiempos, por lo tanto es muy importante mantenernos protegidos ante amenazas externas que son susceptibles desde robarnos información personal hasta atentar contra nuestra integridad física.

- Hay que estar protegidos contra el software malicioso y contra los hackers informáticos. Para esto, hay que contar con un antivirus que se mantenga actualizado todo el tiempo. Existe software antivirus gratuito que se puede descargar de la red, tal es el caso de Avast. (www.avast.com)

    - No ejecutar dos programas antivirus al mismo tiempo, podría ocasionar problemas con el sistema de la computadora.
    - Hay que asegurarse que el programa antivirus que tenemos se actualice constantemente.
    - Es importante escanear constantemente los archivos de nuestras computadoras y mantener encendida siempre la opción de protección activa en el antivirus.
    - El spyware es otro tipo de software malicioso que busca robar la información que se encuentra en nuestros equipos de cómputo. Se recomienda el uso de Spybot (http://www.safer-networking.org/), un programa que identifica y elimina ciertos tipos de malware que ocasionalmente los antivirus ignoran.

- Una medida importante de protección es evitar conexiones no confiables a la red.
  - Instala programas esenciales, que provengan de fuentes confiables.
  - Desconecta tu computadora de internet cuando no la estés utilizando.
  - No compartas tus contraseñas.
  - Mantén actualizados tus programas.

- La protección desde el punto de vista físico de la información es igualmente importante. Asegúrate que la información que tienes en memorias USB, CD's, DVD's, o discos duros externos permanezcan en un lugar seguro. Mantén tu computadora portátil contigo.

- Un recurso de seguridad muchas veces infravalorado, pero que es importante es el uso de contraseñas seguras.
  - Debe ser larga
  - Debe ser compleja
  - Debe ser práctica
  - No debe ser personal
  - Debe mantenerse secreta
  - Debe renovarse constantemente

  Keepass es un programa muy útil en tanto que nos permitirá crear contraseñas complejas sin la necesidad de memorizarlas, ya que dentro del mismo programa, las podemos gestionar. (http://keepass.info/)

- El almacenamiento de información sensible puede representar un riesgo para ti y para las personas con las que trabajas. La encriptación de archivos es una manera de mantener seguros los documentos sensibles de nuestra computadora. El cifrado reduce el riesgo, pero no lo elimina. TrueCrypt (http://www.truecrypt.org/) es un programa diseñado para hacer éste tipo de almacenamiento lo más sencillo posible.

- En caso de que desees recuperar archivos e información que considerabas perdida, que fue borrada intencionalmente o por accidente, lo puedes hacer. Puedes utilizar el software Cobian Backup (http://www.cobiansoft.com/index.htm) para hacer respaldo de tus archivos de manera muy sencilla y automática; y el Undelete Plus (http://undeleteplus.com/) para restituir archivos que fueron borrados recientemente.

- Por otra parte, si lo que deseas es eliminar información de manera permanente, es importante utilizar el software adecuado, que garantice un borrado íntegro, ya que eliminar archivos de la papelera de reciclaje no implica que desaparezcan al 100%. Puedes utilizar el programa gratuito CCleaner (http://www.piriform.com/ccleaner)

- Es muy relevante mantener segura tu comunicación en internet.
  - Se debe utilizar una cuenta de correo electrónico segura, Gmail lo hace, actualmente es uno de los servidores más recomendados en cuanto a seguridad. Así mismo es recomendable el servicio de correo ofrecido por RiseUp.
  - Siempre que navegues en internet, verifica que sea una dirección HTTPS, por ejemplo: https://gmail.com.

Relatoría elaborada por Eduardo Sierra Romero