Serie: hojitas de conocimiento
Tema: SEGURIDAD
Enfoque: Público en general

Una mirada a la seguridad informática

autor:
Hugo Scolnik*

Doctor en Matemática

Experto Internacional en Criptografía y Seguridad Informática

Creador del Departamento de Computación (Fac. Ciencias Exactas - UBA) y actualmente Profesor Consulto Titular

Recibió importantes reconocimientos (*)

En el año 2011 el Gerente General de una empresa multinacional estadounidense especializada en productos y servicios relacionados con Internet afirmó que *"la Humanidad creó, hasta el año 2003, tanta información como la que en este momento se genera en dos días"*. Y para finales de esta década se estima que habrán unos 22.000 millones de dispositivos conectados a Internet.

Para vivir en el mundo actual usamos PCs, notebooks, smartphones, tablets, entre otros dispositivos, pero debemos afrontar múltiples problemas de seguridad causados por virus, troyanos, gusanos y otros malwares; son programas maliciosos que pueden tener como objetivo destruir archivos, robar datos, colocar avisos no deseados, usar tu PC para mandar spam, etc. Estos programas pueden llegar a través de imágenes, sitios peligrosos o cookies (pequeños programas que se almacenan en el navegador que usamos). Los cookies guardan información de la combinación usuario-PC-navegador, con la idea de facilitar la navegación por la web, pero también informan sobre nuestra historia en la web, pueden almacenar programas espías, etc. El usuario puede permitir los cookies, bloquearlos o eliminarlos usando las opciones del navegador, pero muchos sitios no funcionan si no los habilitamos.

La solución es usar un antivirus y/o programas de detección de malware. Hay varios excelentes y gratuitos, pero se entiende que eventualmente pueden fallar. Por ejemplo, si el antivirus se actualiza a las 10 a.m. y aparece un nuevo virus un minuto después, el mismo no será detectable hasta la nueva actualización. Por eso, conviene hacer un escaneo periódico de todo el equipo, pues con seguridad aparecerá algún virus escondido en alguna parte.

SISTEMA OPERATIVO: El sistema operativo (SO) de una computadora es un conjunto de programas que permiten al usuario interactuar con el hardware (CPU o Unidad Central de Procesos, discos, y otros periféricos) en forma "simple", provee servicios a las aplicaciones y administra los recursos disponibles, como la memoria. Es el encargado de realizar tareas fundamentales como manejar dispositivos (teclado, mouse), enviar información a la pantalla para tornarla visible, etc. El SO tiene prioridad sobre cualquier otro programa. Los sistemas operativos más utilizados son Windows, Linux, Mac, DOS[1] y Android, y tal como sucede con los programas usuales, pueden tener errores (bugs) que son explotados por los hackers[2] para ingresar a los sistemas. Por dicha razón los proveedores generan continuamente nuevas versiones y es muy importante mantener actualizado al SO que utilizamos.

INTRUSIONES: Los hackers intentan penetrar tus dispositivos de muchas maneras distintas. Inclusive pueden usar la cámara de video para espiarte. La solución es tener instalado un cortafuego (denominado "firewall" en inglés). Los hay muy buenos y gratuitos en la web.

ENCRIPTACIÓN DE DATOS: Para proteger tu información sensible lo mejor es encriptar los datos y afortunadamente hay software recomendable y gratuito, tanto para proteger archivos como discos (por ej.: www.truecrypt.org).

ACCESO A SITIOS WEB: Los sitios seguros se identifican por un candadito de color amarillo. Hay que clickear en ellos para comprobar que no sean sólo una imagen y verificar el certifica-

do digital que protege las transacciones con esos sitios. Cuando uno se conecta a un sitio seguro, el certificado digital del mismo que contiene su clave pública se instala en nuestra PC y permite que todo lo que hagamos se encripte usando dicha clave. De ese modo, nuestra información sólo podrá ser descifrada por el poseedor de la correspondiente clave privada, o sea el sitio con el cual nos comunicamos. Este proceso se lleva a cabo mediante un protocolo especial llamado https (HyperText Transfer Protocol Secure). Es interesante observar que ninguna tarjeta de crédito ha reportado fraude en transacciones realizadas a través de sitios seguros pero, sin embargo, al usuario normal le parece que es más confiable entregar su tarjeta a un mozo de restaurant quien tendría la oportunidad de copiar sus datos o clonarla con dispositivos especiales.

MANEJO DE PASSWORDS: La gran mayoría de los problemas de seguridad se generan por el uso de contraseñas inseguras. Esto es lógico pues para operar con mails, bancos, etc., debemos memorizar una gran cantidad de ellas. Es por eso que recurrimos a emplear claves basadas usualmente en nombres propios, cumpleaños u otros datos memorizables. De hecho, no se nos ocurre usar algo mas seguro como ser: hY&%0!!"€€@#Uzj398\ñ/. La mejor solución es recurrir a un programa para administrar claves[3]. En la Web se pueden encontrar varios disponibles, eficientes y sin cargo. El mismo exige memorizar una sola clave maestra, e internamente se pueden almacenar todas las claves que se necesiten, incluso el programa mismo las puede llegar a generar. No importa que sean difíciles de recordar dado que con un click se las copia al portapapeles para emplearlas donde se necesiten. Es importante destacar que hay de dos tipos: los que se comunican con la web y los que no. Los primeros deben evitarse en temas que requieran máxima seguridad. Algunos ofrecen el "auto-rellenado de formularios" y para ello almacenan en la web nuestros datos básicos, lo cual puede considerarse como algo no recomendable.

USO DE CELULARES Y Wi-Fi[4]: Lo primero que se debe saber es que los celulares son radios, y por lo tanto las conversaciones se pueden monitorear con un scanner, excepto que estén encriptadas. Un tema importante es que los teléfonos inteligentes tienen normalmente activado un GPS y por lo tanto somos "geolocalizables". Con respecto al Wi-Fi, habría que evitar las redes abiertas no seguras y por sobre todo, no realizar jamás a través de ellas operaciones sensibles como el "home banking". Los esquemas de seguridad han evolucionado y lo conveniente sería usar WPA2 como protocolo de acceso para el Wi-Fi ya que emplea AES, un algoritmo moderno de encriptación que es más seguro.

BORRADO INSEGURO DE ARCHIVOS: Como es sabido, el simple borrado de un archivo no lo destruye físicamente. El sistema operativo solamente marca como "utilizable" el sector de disco donde el mismo está grabado, pero la información existirá hasta que no se le grabe encima nueva información. Lo más seguro, al menos para el mundo civil, es usar el borrado seguro. Esto consiste en sobreescribir el área de disco correspondiente con bits aleatorios una cierta cantidad de veces. Este proceso se denomina "wiping" en inglés y en Internet hay varios productos disponibles.

USO DE MAIL: Los mails presentan diversos problemas de seguridad y la mejor manera de protegerlos es usando certificados digitales que permiten, si el destinatario también posee uno, encriptar el contenido. Otra posibilidad es escribir un documento, encriptarlo con una clave secreta, y mandarlo como adjunto de un mail normal. Como otra medida de seguridad los "webmails" más populares ocultan la dirección IP del remitente con el objeto de evitar su identificación.

PROCESANDO EN LA NUBE ("cloud computing"): Hay proveedores a nivel mundial que ofrecen sitios con software de aplicación actualizado, controles de seguridad al nivel requerido y con mucho espacio físico para procesar toda la información que necesitemos. Para preservar nuestra privacidad se utilizan mecanismos de encriptación de datos. Realmente la informática debería llegar a ser accesible como la electricidad o el gas, donde el usuario final se desentienda de las actualizaciones y de los virus (temas que están a menudo fuera del alcance de la mayoría de las personas) para concentrarse solo en lo que necesita hacer. La computación en la nube apunta justamente a ofrecer eso.

(*) ALGUNOS RECONOCIMIENTOS RECIBIDOS POR EL AUTOR:
En 2003: Premio Konex Ciencia y Tecnología
En 2014: Doctorado Honoris Causa - Universidad Nacional de Cuyo

HUMOR GRÁFICO
Gentileza del humorista argentino TUTE.
www.tutehumor.com.ar
www.facebook.com/Tute.dibujante

REFERENCIAS
1 Se utiliza actualmente para ejecutar programas en modo comando.
2 En la actualidad, este término se usa de forma corriente para referirse mayormente a los criminales informáticos.
3 Cumplen la función de "free password manager".
4 Red de comunicación inalámbrica.

Publicación a cargo del Dr. Daniel Pasquevich y la Lic. Stella Maris Spurio.
Comité Asesor: Ing. Hugo Luis Corso - Ing. José Luis Aprea.
Responsable Científico: Dr. Gustavo Duffó.
Versión digital en www.cab.cnea.gov.ar/ieds

Instituto de Energía y Desarrollo Sustentable
Comisión Nacional de Energía Atómica
Tel: 011-4704-1485 www .cnea.gov.ar/ieds
Av. del Libertador 8250 - (C1429BNP) C. A. de Buenos Aires - República Argentina
Año de edición: 2016 **ISBN: 978-987-1323-12-8**