Consejos Técnicos

¿Cuanta de su información personal está disponible en Internet?

Por Antonio Hernandez

En el Boletín de enero de 2017 publiqué el artículo "Crímenes cibernéticos y la salud de su computador" en el que se dieron recomendaciones sobre cómo proteger los computadores y las redes para prevenir los ataques de los "hackers".

También se dieron una serie de sugerencias que se resumen a continuación:

- *Sea cuidadoso con los programas de distribución gratuita que están disponibles en la Internet, tales como las cuentas de correo electrónico gratuitas. A cambio de estos servicios gratuitos, usted está regalando su información personal! Esta información, generalmente, es usada o vendida para fines de publicidad.*
- *Es más fácil para los hackers penetrar los sistemas y computadores que usan programas gratuitos. La razón es que estos programas tienen menos barreras de protección incorporadas.*
- *Siempre tenga presente que en el espacio cibernético usted no es el USUARIO, usted es el PRODUCTO y su información personal es una mercancía.*
- *Si quiere mantener una información en secreto o privadamente, **nunca** la suba o la envíe via Internet. La información permanecerá para siempre en el espacio cibernético. Especialmente sea cuidadoso con la información que envía o sube en las redes sociales.*

En el mismo artículo se escribe sobre una nueva clase de crimen cibernético del grupo de los virus "malware" y específicamente el denominado "ransomware". Este virus, una vez que se activa, encripta los datos del computador y bloquea el acceso a la información hasta que se paga un rescate.

El primer motivo para recordarles este tema de la vulnerabilidad de los computadores y los crímenes cibernéticos es debido a que las intromisiones y ataques a los computadores se han incrementado últimamente. Es muy probable que hayan oído del reciente ataque a computadores, a nivel mundial, del virus "ransomware" llamado 'WannaCry" que atacó simultáneamente sistemas corporativos de computadores en más de 150 países y afectó a más de 200.000 personas. Hospitales, grandes empresas y oficinas de gobierno fueron algunas de las instituciones más afectadas. El virus se propagó aprovechando una vulnerabilidad del sistema operativo Windows. Un parche o programa de seguridad para corregir esta vulnerabilidad se puso a disposición de los usuarios en el mes de marzo. Este programa de corrección también incluyó versiones del sistema operativo Windows que han sido descontinuadas (XP, Vista, 7 y 8). **Si no han actualizado sus computadores o sus redes con este parche de seguridad, sus computadores son vulnerables y están en riesgo de ser infectados.** El costo del rescate solicitado es del orden de los US $300 pagado en BITCoins (moneda digital).

El segundo motivo fue generado por un artículo reciente del ‘Wall Street Journal” referente a cómo las personas reaccionan ante los riesgos de la conexión en Internet a su privacidad y los trucos y mecanismos usados para recolectar y almacenar la información personal que la convierten en “un libro abierto en la red”.

Se ha llegado al punto en que toda la información individual es vulnerable, desde la más insignificante hasta la más crítica. Esta información personal puede ser usada para acosar, chantajear o interrumpir la operación normal de su computador. En resumen, Su información puede ser convertida en un arma que pueden usar para atacarlo.

En el espacio cibernético hay grupos denominados agregadores de datos que están especializados en recolectar datos usando “bots” (programas robot que son aplicaciones que funcionan en forma automática y repetitiva recolectando información a una velocidad más alta de lo que podría hacerlo una persona). Los bots recolectan cualquier información y toda la que esté disponible a cerca de usted, desde sus hábitos de navegación en Internet hasta sus contactos y el contenido de los correos electrónicos. Esta información es acumulada en archivos para ser utilizada de diferentes formas tales como enviarle publicidad sobre productos y servicios que usted busca frecuentemente en Internet o para atacarlo a usted o a su información financiera. Esta situación se vuelve realmente crítica cuando la información que está segmentada y proviene de múltiples fuentes es agrupada, analizada y sintetizada usando herramientas para análisis de datos.

Aunque las plataformas de las redes sociales tienen controles de privacidad, el problema está en que las personas tienden a no usar estos controles o no saben cómo hacerlo. Por otra parte, hay disponibles en la Internet programas de dominio público, con funciones de búsqueda, que facilitan o permiten buscar y acceder a los mensajes en plataformas como Facebook.

Por otra parte, hay que tener en cuenta que aun si usted remueve o borra su información en una plataforma de redes sociales o cancela su cuenta, usted no puede borrar la información enviada o almacenada por otros.

Adicionalmente a las sugerencias y recomendaciones que se han suministrado, quiero agregar una última relacionada a las “cookies” (pequeños archivos de texto creados por los dueños de portales de Internet o sitios web, que son almacenados en el computador del usuario en forma temporal o permanente, para permitir y facilitar que el sitio de Internet lo reconozca y guarde información sobre sus preferencias y gustos). Tenga cuidado con los sitios de Internet que le piden que acepte “cookies”. Aplique su buen criterio al aceptar o rechazar estas solicitudes. No todas las cookies son malas, pero hay que tener en cuenta los riesgos de vulnerabilidad y privacidad.

En resumen, el espacio cibernético contiene más información a cerca de usted de lo que usted piensa, y esta información está permanentemente disponible para quien la busque dando su nombre y otras palabras clave que lo identifiquen, como su lugar de trabajo o actividades en las que ha participado. Si no lo ha hecho todavía, usted puede intentarlo y se sorprenderá se la cantidad de información acerca de usted que puede obtenerse.