Consejos Técnicos

Crímenes Cibernéticos y la Salud del Computador

Por Antonio Hernández

El ataque malintencionado a computadores y redes ha aumentado dramáticamente en los últimos diez años. Aunque esta situación no es nueva, lo que sí es nuevo es el daño que estos ataques pueden ocasionar al usuario. En los inicios del uso de los computadores personales, los archivos en los disquetes y los discos duros podían se infectados fácilmente con "virus" que actuaban de diferentes formas e interrumpían la operación de los computadores. La transmisión se daba por el uso o activación de archivos infectados y aunque la contaminación obstruía la operación normal del computador, esto podía se corregido fácilmente usando programas para eliminar los virus e inmunizar los computadores. En la mayoría de los casos, esta infección con virus no era crítica para la operación del computador y generalmente no comprometía la integridad y el bienestar de los usuarios.

La conexión de computadores en redes, el uso de Internet y el uso de programas para la búsqueda de información, la amplia popularidad y uso del correo electrónico como el mecanismo preferido para comunicarnos, ha abierto el campo para nuevas y más letales formas de intrusión en los computadores y las redes. Estas nuevas amenazas no solo incluyen a los computadores y las redes sino que también pueden comprometer la integridad personal y las operaciones financieras de las personas y los negocios.

El riesgo de los ataques se ha incrementado a causa de las diferentes clases de plataformas móviles o dispositivos que intercambian información con los computadores, y al amplio uso de las redes sociales para intercambiar o comunicar información. Muchas veces esta información es personal y privada. Recuerde bien, que todo lo que usted coloca en un portal o página de Internet y todo correo electrónico que es enviado puede ser obtenido o leído por expertos en computación llamados "hackers" o piratas cibernéticos, y el riesgo es mayor ya que toda esa información queda permanentemente en el espacio cibernético.

En el pasado los computadores con sistema operativo de Windows fueron el objetivo de los ataques con virus en razón de su amplio uso en el mundo de los negocios. Hoy los ataques con virus también afectan a los computadores con sistema operativo de Apple. Los computadores con sistema operativo de Linux tienen menor riesgo de ser objeto de cierta clase de ataques directos.

Para ilustrar el riesgo y los potenciales daños que los ataques pueden ocasionar en los computadores, las redes, los negocios y las personas, a continuación, se presentan diferentes categorías de ataques basados en el objetivo de los mismos y el resultado o daño que ocasionan. Algunos de los ataques se realizan mediante contaminación con virus y otros se realizan mediante el uso de tácticas de "Ingeniería Social".

Ingeniería Social, en el contexto de los computadores y de la seguridad de la información, se refiere a la manipulación psicológica de las personas para hacerlas divulgar información confidencial tales como cuentas, nombres de usuario y códigos y contraseñas de acceso a cuentas en Internet, detalles

de tarjetas de crédito o números de cuentas bancarias, identificación personal o número del seguro social.

Estas formas fraudulentas de obtener información pueden ser realizadas mediante el uso del computador (principalmente por el correo electrónico) o por otros mecanismos tales como llamadas telefónicas.

En computación, una forma común de ingeniería social es la denominada “phishing” o fraude electrónico. El phishing es el intento de obtener información sensible, generalmente con intención maliciosa, engañando al interlocutor mediante una comunicación electrónica que parece verdadera o fidedigna. El phishing se hace generalmente a través del correo electrónico o de mensajes de texto. Solicitan que se suministre la información personal a un portal o sitio de Internet que luce idéntico al sitio verdadero que es conocido por el interlocutor. La mayoría de los sitios o portales falsos se relacionan con instituciones o transacciones financieras y el objetivo es robarle el dinero. Algunas veces es muy difícil diferenciar entre el sitio verdadero y uno falso. Si usted no está seguro que el sitio es el verdadero no dé la información solicitada. En su lugar, contacte la institución y confirme si la solicitud de información proviene de ellos.

Además de los virus de computador ya mencionados al principio, hay una nueva generación de virus llamados “malware” o programas maliciosos. La diferencia con los primeros, es que además de afectar o interrumpir la operación del computador, el virus intruso junta y roba información sensible a la vez que trata de ganar acceso a los sistemas del computador, y enviar publicidad no deseada. Uno de los robos de información más comunes es el directorio de contactos del correo electrónico con la intensión de usarlo para enviar publicidad o mensajes no deseados. Algunas veces, su computador y la secuencia de letras y caracteres tecleados pueden ser espiados por periodos largos de tiempo. Otras veces, el virus puede ocasionar daño o sabotear la operación del computador. En algunos casos, el virus se puede replicar e infectar otros archivos o programas o corromper la información. Es muy importante tener el computador y la red protegidos para que tales intrusiones puedan ser detectadas. El sistema operativo Windows 10 tiene incluidas herramientas para proteger contra los ataques de virus. Este grupo de programas es conocido como “Grupo para la Defensa de Windows”. Una vez activado el programa actualiza periódicamente la tabla de virus y escanea el sistema en forma automática para eliminar los virus. También hay programas comerciales para limpiar y proteger de virus el computador.

En Internet hay varios programas para proteger contra ataques de virus que están publicitados y accesibles en forma “gratuita”. La realidad es que estos programas no son totalmente gratuitos, ellos son ofrecidos bajo un modelo de negocio conocido como “freemium” (contracción de las palabras free y premium). Solo una porción del programa es gratis (free) y hay que pagar (premium) por el resto del programa si se quiere usarlo en toda su capacidad.

Uno de los tipos más peligrosos de virus maligno es el llamado “ransomware”. Una vez que el virus es activado, ejecuta una “virología-críptica” que encripta la información del computador dejando bloqueado el equipo hasta que se pague un rescate. La información en el computador permanecerá bloqueada hasta que la suma de dinero solicitada es pagada. Esta forma de crimen cibernético ha pasado de los computadores personales los computadores y sistemas empresariales.

Durante 2016 varios hospitales en los Estados Unidos de América fueron infectados con este tipo de virus y ellos pagaron el rescate solicitado para poder recuperar la información y continuar trabajando.

A continuación se dan algunas recomendaciones para proteger su computador:

- Siempre use contraseñas fuertes en sus cuentas. Incluya mínimo ocho caracteres: use letras mayúsculas y minúsculas, números y caracteres especiales.
- Evite usar la misma contraseña en varias cuentas. Los piratas cibernéticos son conscientes de esta práctica.
- No guarde en su computador archivos que contengan las claves y contraseñas. Guarde esta información en un sitio seguro.
- No comparta con otros sus contraseñas.
- Cuando entre a sus cuentas o sitios personales en Internet (log-in), particularmente a los que manejan información financiera, asegúrese que sale del sitio (log-out) una vez termine la sesión o transacción.

Reflexiones finales:

- Sea cuidadoso con los programas que obtiene de forma gratuita en Internet tales como cuentas de correo electrónico gratuitas. A cambio de estos servicios usted está entregando de forma gratuita su información personal! Esta información puede ser vendida o usada para fines publicitarios.
- Los programas gratuitos son de más fácil penetración para los piratas cibernéticos, la razón es que tiene menos niveles de protección.
- Siempre sea consciente de que en el espacio cibernético usted no es el USUARIO, usted es el PRODUCTO. Su información es una Mercancía.
- Si usted quiere tener algo en secreto o privado, **nunca** lo suba o lo envíe vía Internet. La información permanecerá para siempre en el espacio cibernético, aunque usted la borre. Sea especialmente cuidadoso de lo que usted publica en portales de redes sociales.