Ciencia y TECNOLOGÍA

Cero popularidad de Monedas digitales

La presencia de las monedas virtuales como el bitcoin en México ya es una realidad y el gran reto que queda para popularizarlas es encontrar soluciones o aplicaciones que simplifiquen su uso, en particular como una forma de medio de pago o en remesas. Los mexicanos que viven en el extranjero al momento de enviar dinero pagan hasta 10 dólares de comisión, lo cual merma los recursos, mientras con la moneda virtual no sólo bajaría sino que sería más fácil porque los recursos se pueden mandar por internet.

MUNDO DIGITAL

Seguridad Informática

Las contraseñas de los dispositivos de tecnologías de la información y comunicación (TIC) deben ser personalizadas; no dejar las que ofrece el proveedor

Sergio J. Castro*
scastro@cetys.edu.mx

Foto: Cortesía

El éxito de la seguridad informática depende del usuario.

El pasado 9 de junio se publicó en los diarios canadienses y se diseminó a través de Internet, que un par de jóvenes de apenas 14 años lograron el acceso a un ATM (Automatic Teller Machine, cajero automático) utilizando la contraseña que por omisión se le asigna al ATM cuando sale de fábrica. Estos jóvenes encontraron en línea el manual del ATM y decidieron probar con uno del Banco de Montreal. Se sorprendieron cuando la contraseña funcionó. Los jóvenes advirtieron al banco de la situación.

Dejar la clave de seguridad que por omisión se le asigna a un cajero automático, o a cualquier dispositivo tecnológico, que desafortunadamente es una práctica muy común, habla muy mal de las políticas informáticas y del equipo de seguridad del Banco de Montreal.

CLAVE, POR DEFAULT

Los dispositivos de tecnologías de la información y comunicación (TIC) necesitan ser configurados por quien los adquiere para ajustarlo a sus necesidades y a sus políticas internas. Para poder entrar a estos dispositivos los fabricantes asignan por lo general un usuario y una contraseña que aplica a todos su línea, el más común tanto para usuario como contraseña es la palabra "admin". También por lo general todo fabricante recomienda que inmediatamente se cambien estos valores. El Banco de Montreal no lo hizo.

La recomendación de los fabricantes aplica tanto para empresas como para usuarios finales que compran dispositivos de las TIC para el hogar; dispositivos como enrutadores o puntos de acceso a redes Wi-Fi, o cámaras IP, teléfonos VoIP (Voz sobre el Protocolo de Internet), computadoras personales, tabletas y teléfonos móviles. Vaya, hasta el NIP del buzón de voz debe de ser cambiado.

Por más eficaces y complicados que sean los mecanismos de seguridad son estériles si el usuario final no los aplica. El 10% de la seguridad informática depende de la tecnología que se implemente y el 90% depende del usuario final. Usuarios como Usted y yo. Por ejemplo, el candado de la puerta representa el 10% de la seguridad en su hogar. El que usted lo cierre, se asegure de que la puerta quede bien cerrada, y el mantener un control estricto de las llaves que abren ese candado representa el 90% de la seguridad en casa.

La contraseña no es el único mecanismo de seguridad. Existen personas mal intencionadas que buscan vulnerabilidades para entrar a sus sistemas informáticos y robarse información personal como contraseñas, cuentas de banco y NIPs (Número de Identificación Personal) para posteriormente robarse la identidad y así robar dinero. Existe software denominado "malware" o "spyware" que llega a los usuarios a través de correo electrónico y se auto instala y se ejecuta de manera silenciosa e invisible en el fondo de su PC, corriendo concurrentemente con los programas que el usuario está ejecutando de manera voluntaria.

Estos programas malignos pueden llegar como "Spam" o como correspondencia electrónica que aparenta ser de alguien a quien el usuario conoce, este alguien puede ser una institución con la cual el usuario tiene una cuenta, como un banco o una compañía de telefonía, a esto último se le denomina "phishing", o pescando incautos.

En las TIC es muy importante ser desconfiado. El perder información personal es uno de los males. Otro de los males es perder toda la información en el equipo de cómputo. El que se instale un virus puede ocasionar que se pierdan muchas horas de trabajo.

NIP PERSONALIZADO

Las recomendaciones son básicas. Cambie las contraseñas de sus dispositivos, no utilice las que vienen de fábrica, si alguien puede entrar a su cámara IP y ver las imágenes dentro de su hogar lo hará. Utilice contraseñas difíciles de adivinar, entre más complicadas mejor. Algunos sistemas permiten utilizar los caracteres especiales como %$&*#@, si puede utilícelos. También se recomienda cambiar las contraseñas constantemente, por lo menos una vez al año.

En enrutadores y puntos de acceso Wi-Fi se recomienda utilizar encriptación, si tiene la opción WPA2 utilice ese algoritmo de encriptación, por el momento es el mejor.

Con respecto a correos electrónicos mucho se ha repetido ejercer precaución, no abrir los archivos anexos si no conoce a quien los envía, sobre todo si son archivos ejecutables. También se recomienda no responder a personas que desde África envían información no solicitada ofreciendo oportunidades muy lucrativas.

La seguridad informática es en nuestros días un tema que involucra a todos, ya que estamos entrelazados con muchos proveedores que nos brindan sus servicios a través de las TIC; y el tener cuenta que a estos proveedores les estamos confiando información, muchas veces confidencial. Pero a nadie le interesa más la seguridad personal que a uno mismo. La precaución es la mejor seguridad, en nuestras manos está el 90% de ella.

*El autor es licenciado en ciencias computacionales por la UABC, cuenta con maestría en redes y telecomunicaciones por Cetys Universidad. Ejerce en la iniciativa privada.