Riesgos en el uso de internet

A continuación, le presentamos algunos de los fraudes más comunes que están siendo o han sido utilizados por los defraudadores en los diversos sitios de Internet y que pueden representar un riesgo para usted. Para evitar este tipo de riesgos, contamos con una sección Recomendaciones de seguridad de nuestra página web www.bansi.com.mx en el apartado Seguridad, que le pueden ser de utilidad en su navegación y operación bancaria por internet.

PHISHING

El término se asemeja al inglés fishing (pescando). Se llama así a la práctica fraudulenta de conseguir información confidencial, enviando un correo electrónico haciéndose pasar por una institución o agencia del gobierno con el propósito de que los receptores lo contesten o lo reenvíen con información real. Estos correos se envían en forma masiva esperando que algunos los contesten pensando que se están comunicando con su institución financiera y entreguen, en realidad, a los defraudadores información confidencial, tal como clave de usuario, número de cliente, número de cuentas, password o PIN. Utilizan frases como “estamos actualizando nuestros registros”, “seguridad y mantenimiento”, “investigación de irregularidades”, “personalización de cuentas”, “su cuenta ha sido congelada”, “tenemos que reconfirmar sus datos”, “su tarjeta de crédito ha sido cancelada”, “actualice sus datos”. Lo anterior, es para lograr convencerlo de proporcionar sus datos.

KEYLOGGERS

Son dispositivos físicos (conectados entre la PC y el teclado) y programas que se instalan en las computadoras que tienen como fin almacenar en un archivo todo el texto que se digita en un teclado. Posteriormente, este archivo es recuperado con el fin de conocer toda la información que el usuario digitó, incluyendo sus identificadores de usuario y contraseñas. El riesgo es mayor si utiliza equipos públicos de Internet (cafés Internet, hoteles, de otro usuario) o si alguien más tiene acceso físico a su computadora.

WEB PAGE SPOOFING

Son sitios web con dirección y apariencia similares a las de una institución o empresa, que buscan que el usuario proporcione sus datos personales (como su nombre de usuario o contraseña) al tratar de ingresar mediante los campos de acceso usados regularmente. Por lo general, es más fácil confundirse y acceder a estas páginas fraudulentas al tratar de llegar al sitio real mediante ligas colocadas en páginas de “concentradores de información” o de terceros en general.

SPYWARE

Es un tipo de programa o software que envía a terceros su información personal sin su autorización o conocimiento. El tipo de información que se envía comprende los sitios web visitados, nombres de usuario, contraseñas. La información puede ser utilizada para hacer mal uso de ella, y en algunos casos para enviarle publicidad. Generalmente, este programa se carga en las computadoras al abrir o “bajar” de Internet programas de distribución ilegal o de uso gratuito.

Riesgos en el uso de internet

ADWARE

Es el software que muestra publicidad en su equipo. Se trata de anuncios que aparecen de repente en su pantalla en ventanas emergentes (pop ups o banners). El riesgo de este tipo de programas reside en que en ocasiones incluyen software Spyware sin que esto sea del conocimiento de quien lo instala. Tanto el Adware como el Spyware se instalan sin permiso en su equipo, engañándolo con botones que dicen realizar alguna función (descarga de juegos, premios, videos gratis o programas), o bien pueden incluirse en programas para compartir archivos por Internet. Muchos de los programas de software gratuito disponible en Internet incluyen Adware y Spyware.

VIRUS

Son programas que se instalan en su computadora y que realizan tareas orientadas a la pérdida de información o al uso inadecuado de los recursos de su computadora. Estos programas pueden venir adjuntos a archivos ejecutables, juegos, imágenes, scripts de páginas web, e instalarse sin que usted se dé cuenta, hasta que se ejecuten y causen daño o pérdida de información. Pueden reproducirse y transmitirse en varias computadoras mediante correos, juegos y archivos ejecutables en general. Una variante son los denominados ‘gusanos’ (worms), que no tienen la capacidad de reproducirse, o los ‘caballos de Troya’ que se adjuntan a archivos válidos y esperan un tiempo o acción definida para activarse.

SECUESTRO DE SESIÓN

Cuando usted trabaja en una computadora conectada a red, ya sea en su trabajo o en lugares públicos, el administrador de ésta puede habilitar una funcionalidad en su equipo para permitir “tomar el control” de su sesión, o bien, monitorear su sesión, con lo que puede observar en su pantalla lo mismo que usted en la suya. De este modo puede hacerse de información valiosa que usted ingrese en las aplicaciones, páginas web y correos.