BOLETÍN No. 044 –>>

Personas que suelen usar tarjetas de crédito para realizar compras vía web o transferencias bancarias deben verificar que la página electrónica cuente con *certificado SSL*.

Empresas requieren realizar al menos dos veces al año auditorías de ciberseguridad.

La mensajería instantánea está siendo el nuevo blanco para el robo de datos e información confidencial por parte de los hackers, sin embargo, estos ataques se realizan a nivel servidor web y no de manera personal, por ello, los usuarios deben mantener privado cualquier dato del cual puedan ser víctimas de cualquier ataque; así lo aseguró Rafael Rogelio Bucio Velázquez, director de la empresa de ciberseguridad TPX.MX al dictar en la Universidad Autónoma de Aguascalientes la ponencia “El hacking a través de los años”, a estudiantes de Ingeniería en Sistemas Computacionales e Informática y Tecnologías Computacionales.

En entrevista previa a su conferencia, comentó que tras el surgimiento de WikiLeaks, organización que se dedicó a filtrar a través de la red documentos e informes de Estados Unidos, se han hecho nuevas leyes para contrarrestar el ciberespionaje, sin embargo, la información en internet no es segura y aunque se usen muchos filtros de seguridad, la información siempre tiene problemas de fuga, por lo que a partir de estos acontecimientos, se revelen datos privados.

En referencia al Día del Internet Seguro, celebrado este 9 de febrero, Bucio Velázquez indicó que para evitar ser víctima de *hackeo*, los usuarios requieren tener una cultura informática, es decir, cuidar las páginas a las cuales desean ingresar y verificar previamente la dirección URL, pues los hackers se dedican a crear páginas clones para sustraer información privada.

Asimismo, recordó que para las personas que suelen usar tarjetas de crédito para realizar compras vía web, revisar estados de cuenta o bien efectuar transacciones financieras, es indispensable verificar que las páginas en donde realizarán estas acciones cuenten con *certificado SSL* (Secure Sockets Layer), es decir, una capa de conexión segura; aunque principalmente recomendó que cualquier movimiento bancario o de compra por internet se lleve a cabo desde una computadora personal, pues es más fácil realizar una sustracción de datos personales desde una unidad que sea disponible para terceros.

En cuanto a la ciberseguridad empresarial, el director de la empresa TPX.MX sostuvo que deben realizar al menos de manera mensual dos auditorías de seguridad tanto física como perimetral, pues hoy en día el hacking no sólo abarca sistemas informáticos, ya que existen aparatos capaces de sustraer datos o intervenir líneas telefónicas, lo cual es también considerado como un tipo de ataque cibernético. Aunado a estas acciones, señaló que la iniciativa privada debe tener a los usuarios con ciertos privilegios para evitar que roben o inserten información en las organizaciones.

Bucio Velázquez comentó que este tipo de auditorías aún no ha permeado a las grandes empresas de México, lo cual permite abrir un campo para futuros egresados de programas de

estudio enfocados a la seguridad informática, pues les será redituable tanto en lo económico como en lo profesional, por lo que invitó a los interesados en desarrollar sus habilidades en la ciberseguridad a obtener certificaciones, conocer vulnerabilidades y aprender idiomas, principalmente inglés y portugués, pues en países donde se hablan estas lenguas hay una mayor oferta de empresas de seguridad web.

Finalmente, calificó al siglo XXI como la década de la revolución de la ciberinformática, pues el concepto de *hacking* ha ido evolucionado con el paso de los años, pues hoy en día se ha ampliado a definir a personas que a través del ingenio, el emprendimiento y la creatividad logran un determinado objetivo que no es necesariamente dañino, sino que puede apoyar a fortalecer la seguridad en internet.


"Pensando como Hacker, Defendiendo como Hacker"
Formando expertos en seguridad de la información.
IPX
uaa