Seguridad en las Redes Sociales

"La seguridad no es un producto, es un proceso" - Bruce Schneier

Reina Camacho
reina.camacho@ucv.ve

Las redes sociales se han añadido al día a día de las personas, las invitaciones a compartir en las redes sociales se multiplican de manera exponencial; en cualquier medio informático nos encontramos que, las empresas, personas, eventos, foros, amigos, etc., nos invitan a conocer más sobre ellos a través de las redes sociales como: Twitter, MySpace, Facebook, Linked ln, Hi5, Google+, entre otras. En el contexto universitario también se observa este comportamiento, la Universidad Central de Venezuela (UCV) nos invita a visitar su cuenta en Facebook llamada "Dialogo UCV" y su cuenta en twitter @dicucv, entre otros.

Las instituciones de educación superior, incluyendo la UCV, han aprovechado algunas de las ventajas que ofrecen estas redes sociales, entre las cuales se destaca la velocidad con que se propaga la información, es decir, hoy en día se puede obtener mucha información sobre cualquier tema en cuestión de minutos. Otras ventajas son la facilidad del acceso a dicha información y la gran cantidad de personas que pueden tener acceso a ella, generando espacios de opinión. Sin embargo, hacer un uso inapropiado o inadecuado de estas redes puede traer consecuencias serias, como por ejemplo: propagar virus en la red, robo de información confidencial, daño a la imagen y reputación personal e institucional, entre otros.

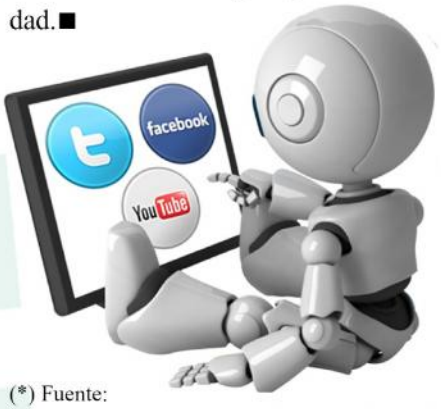
La Empresa de Seguridad Tufin Technologies* realizó una encuesta a 1.000 estudiantes británicos de entre 18 y 21 años, la cual arrojó los siguientes resultados: una cuarta parte de los estudiantes universitarios ha "hackeado" algún sistema informático. De esta encuesta, encontró que un 37% había hackeado perfiles de Facebook, 26% cuentas de correo electrónico ajenas y un 10% cuentas de compras en línea, entre otras actividades. Un tercio lo hace por diversión, 22% por curiosidad y un 15% para hacer dinero.

"Lo que este estudio pone de manifiesto es que el hacking de cuentas personales, ya sea correo electrónico o Facebook está sucediendo con regularidad entre la población estudiantil (…) Vivimos en un mundo donde las redes sociales, el correo electrónico e Internet son parte de nuestra vida diaria a edad temprana, por lo que una educación es esencial para garantizar que los jóvenes conozcan las consecuencias que puede tener esta actividad. El Hacking es ilegal y tenemos que asegurarnos que todo el mundo lo entienda" dijo Stuart Hyde, Presidente de la Sociedad Policial del Ciberespacio.

En Venezuela, el delito de acceso indebido, sabotaje o daño a sistema, incluso violación de la privacidad de

la data o información de carácter personal, está sancionada en la Ley Especial contra los Delitos Informáticos aprobada en el año 2001, penado con prisión y multa; en este sentido, la Dirección de Tecnología de Información y Comunicaciones (DTIC) exhorta a toda la comunidad universitaria a tener conciencia sobre el uso de las redes sociales, y los riesgos que ello implica, e insta a tener en cuenta ciertas recomendaciones al hacer uso de esta tecnología, las cuales ayudarán a proteger su perfil, imagen, incluso su computador, entre otros.

Las redes sociales son un excelente instrumento para facilitar la comunicación entre las personas o grupos de personas, sin embargo se deben utilizar con moderación y responsabilidad.■



(*) Fuente: www.fayerwayer.com/2010/09/un-23-de-estudiantes-universitarios-ha-hackeado-sistemas/

Recomendaciones para un buen uso de las Redes Sociales:

- Se debe pensar bien lo que se va a publicar, y como lo va a publicar ("esclavo de lo que dice") ya que no se puede volver atrás, además que miles de personas tienen acceso a ella y las leerá.
- Diferenciar lo que es público de lo privado.
- Ser cuidadoso con los nuevos contactos.
- Configurar las opciones de privacidad que las redes sociales proveen al usuario, además de mantener en privado sus datos personales.
- No hacer click a todo enlace enviado, ya que puede ser código malicioso.
- No amenazar, ni difamar a través de correo, mensajería instantánea, entre otros.
- Utilizar contraseñas seguras y cambiarlas periódicamente.
- Cuidar su imagen.
- Reportar o denunciar los perfiles falsos.

Instrumentos jurídicos

Para enfrentar la ocurrencia de incidentes telemáticos, delitos informáticos o delitos cibernéticos, Venezuela cuenta con una sólida base jurídica, dispuesta en las siguientes normas: Ley sobre mensajes de datos y firmas electrónicas, de febrero de 2001 (Gaceta Oficial Nº 37.148); Ley especial contra los delitos informáticos, de octubre de 2001 (Gaceta Oficial Nº 37.313), Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (Resorte) y la Ley Orgánica de Telecomunicaciones (Lote).

Informática criminalística

El Estado dispone de otro organismo adscrito a la Superintendencia de Servicios de Certificación Electrónica (Suscerte) para enfrentar los ilícitos informáticos: El Centro Nacional de Informática Forense (Cenif).

Este grupo tiene la responsabilidad de colectar, preservar, analizar y presentar las evidencias relacionadas con la tecnología de la información, que apoyarán las investigaciones judiciales en la materia.

Por esta vía se brinda respaldo técnico a la Fiscalía General de la República, al Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), al sistema judicial y a otros organismos de seguridad. **Fuente: AVN**