

Seguridad en la Red

Por: Andrés Pumarino M.

Probablemente sea usted alguna de las personas que ha recibido un email en el que tiene un mensaje de su ejecutivo del banco donde tiene su cuenta corriente. En este correo, con la imagen institucional de su banco, le solicita que ingrese al link o enlace que va en el mensaje para actualizar sus datos, dirección, número de teléfono y clave secreta, al parecer nada extraño hasta aquí.

Lo relatado corresponde a una acción que se realiza en internet y que recibe el nombre de *"phishing"* que consiste en aprovecharse de la confianza de las personas a través del uso de la técnica de simular el email de instituciones financieras solicitando antecedentes relevantes como clave secreta, cedula de identidad y que luego son utilizadas para acceder a sus cuentas bancarias o tarjetas de crédito, esta es una nueva forma de fraude que nos amenaza y que está presente en internet. Solamente en mayo del 2004 en Estados Unidos se registraron entre 1.000 y 1.200 reportes de *"phishing"*

Por otra parte, el desarrollo de la tecnología permite idear mecanismos para burlar a personas, sistemas informáticos y estándares de seguridad. En la actualidad conceptos como *"wardriving"* que es el método más conocido para detectar las redes inalámbricas inseguras, es el que circula en los medios tecnológicos. Se realiza habitualmente con un dispositivo móvil, como un ordenador portátil o un PDA (agenda electrónica). El método es sencillo: la persona que ejecuta la acción sólo se pasea con el dispositivo móvil y en el momento en que detecta la existencia de la red inalámbrica, se realiza un análisis a través de programas computacionales que pueden ser descargados en forma gratuita de internet. Para evitar la violación a su red, es importante tener una nueva contraseña, con números y que comience y termine con letras, como mínimo debe tener 8 caracteres, un nuevo número IP, nuevo nombre para su red inalámbrica, en fin varias otras alternativas más técnicas que debe tener presente para evitar posibles infiltrados navegando en su ordenador.

Otra acción frecuente es el llamado "*spyware*" o software espía, que no es más que un programa diseñado para seguir el comportamiento de los usuarios, sobre todo cuando se encuentran en Internet. Un estudio reciente de una consultora de Internet encontró casi 30 millones de programas de este tipo en un millón de computadores en EE.UU.

Las aplicaciones de los programas espía recogen y envían información sobre las páginas web que más frecuentemente visita un usuario, o el tiempo de conexión. También suelen capturar datos relativos al equipo en que se encuentran instalados: sistema operativo, tipo de procesador y memoria. Incluso hay algunos diseñados para saber si el software instalado en el equipo es original. La Cámara de Representantes de EE.UU. aprobó un proyecto de ley que prevé multas elevadas para las compañías o individuos que instalen programas espías ("Spyware"). Esta norma prevé una serie de directrices que obligatoriamente deberán cumplir las empresas de software, como solicitar el permiso explícito de los consumidores antes de instalar algunos programas con los que ellas puedan tener acceso a sus datos.

Sin embargo, la duda que se nos presenta ante este tipo de acciones que se generan en la red provienen del mundo jurídico, ¿Cuál es nuestra protección ante semejantes acciones? ¿Están nuestras normas jurídicas preparadas para hacer frente a estas acciones o aun no se ajusta a los cambios tecnológicos? . En Chile existen lo que se denominan Delitos Informáticos, desde junio de 1993 (Ley 19.223) que fija sanciones en contra de quienes cometen los denominados delitos. Dicho cuerpo legal establece que la persona que maliciosamente destruya o inutilice un sistema de tratamiento de información, alterando su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Asimismo, señala que si como consecuencia de estas conductas, se afectaren los datos contenidos en el sistema, se aplicará la pena indicada en su grado máximo. La mencionada ley que tuvo su origen en la necesidad de adecuar la normativa chilena al vertiginoso avance de las tecnologías de la información establece que quien revele o difunda los datos contenidos en un sistema de información, recibirá la pena de presidio menor en su grado medio, sanción que aumentará en un grado si quien incurre en estas conductas es el responsable de cautelar la invulnerabilidad del sistema. La doctrina señala que no estamos frente a "nuevos delitos", sino ante nuevas formas de ejecutar las conductas típicas tradicionales.

Actualmente se está tramitando en el Congreso Nacional una modificación en el Código Penal con el objeto de adecuar en los tipos penales tradicionales, las nuevas formas delictivas surgidas a partir del desarrollo de la informática, nuestro cuerpo normativo requiere adaptarse prontamente a normas que protejan y sancionen frente a la amenaza de estas nuevas técnicas para cometer delitos, el derecho no puede quedar atrás ante el avance de la tecnología, fundamentalmente si se aspira dar mayor confianza y protección al comercio electrónico.