TP2 – Delitos informáticos

Delito informático: HACKER

Hackear es ser experto en alguna rama de la tecnología, a menudo informática, y dedicarse a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

Evitar/prevenir hackeo:

**1)** Sea consciente de los datos que comparte. No tiene que borrar su perfil en Facebook o en Twitter para estar a salvo, pero les facilita la tarea a los hackers si en las redes sociales publica fechas de nacimiento, películas favoritas o el nombre de soltera de su mamá, datos que a menudo utiliza para contestar las preguntas de seguridad que le dan acceso a sus cuentas online o por teléfono.

**2)** Elija contraseñas complicadas. A un hacker le puede llevar tan solo 10 minutos descifrar una contraseña formada por seis letras minúsculas, pero algunos sitios gratuitos como safepasswd.com lo pueden ayudar a crear una contraseña casi inviolable que combine letras mayúsculas, símbolos y números. Usar frases como contraseñas también suele funcionar (el sitio passphra.se/es lo puede ayudar a crearlas). A un hacker podría llevarle meses descifrar la frase “diga no a los ciberladrones”, por ejemplo, al menos haste este momento.

**3)** Use la verificación en dos pasos. Esta es una función de seguridad que, una vez activada, le solicita que introduzca dos contraseñas para entrar a su cuenta: su contraseña normal y un código que esas empresas le envían en un mensaje de texto a su celular. “El paso adicional representa un leve inconveniente, pero vale la pena cuando la alternativa es ser víctima de un hacker”, señala Matt Elliot, escritor de tecnología del sitio cnet.com. Para establecer la verificación en Gmail, haga clic en Cuenta y luego en Seguridad. En Facebook, inicie la sesión, haga clic en el ícono inferior junto a Página Inicial, y después en Configuración de la Cuenta, Seguridad y Aprobaciones de Inicio de Sesión.

**4)** Use con moderación los puntos de acceso Wi-Fi. Los principales proveedores de Internet inalámbrico público gratuito (un servicio disponible en puntos de acceso situados en cafeterías, aeropuertos y hoteles) no requieren un encriptamiento de los datos que circulan entre Internet y las laptops, lo que implica que cualquier información —como su contraseña de correo electrónico o su estado de cuenta bancaria— es vulnerable a los hackers. En una PC, haga clic en el ícono de conexión inalámbrica en la barra de tareas para desactivarla. En una Mac, haga clic en el ícono de Wi-Fi en la barra del menú para desactivar Wi-Fi.

5) Resguarde su información. En cuestión de minutos, los hackers pueden borrar de su computadora los mensajes electrónicos, las fotografías, los documentos y la música que ha atesorado por muchos años. Proteja sus archivos electrónicos utilizando alguno de los sistemas de resguardo sencillos y gratuitos disponibles en Internet; por ejemplo, crashplan.com y dropbox.com.