UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

CENTRO DE EDUCACIÓN CONTINUA

“La seguridad en Internet. Los portales del sistema bancario.”

(Reportaje)

TRABAJO PROFESIONAL QUE EN LA MODALIDAD DE

TESINA

PRESENTA:

Miriam Montserrat Gómez Mancera

ASESORA: LILIA RAMOS ORDÓÑEZ

CIUDAD UNIVERSITARIA, AGOSTO 2010

Entonces entenderás justicia, juicio y equidad, y todo buen camino. Cuando la sabiduría entrare en tu corazón, y la ciencia fuere grata a tu alma, la discreción te guardará; te preservará la inteligencia. (Pr 2:10-11)

Dedico este trabajo a mis padres, Juan Carlos y Rosalba, y a mis hermanos Carlos, Karla y Mariana, por su apoyo constante y el cariño que nos mantiene unidos pese a nuestras marcadas diferencias. A todos y cada uno de los miembros de mi familia, por ser el aliento para concluir esta etapa de mi vida.

A mis amigos y compañeros, que forman parte de esta historia. Aunque en una cuartilla no pueda nombrarlos a todos, saben de manera personal quiénes son.

Gracias por las sonrisas, los consejos, las discusiones, los regaños, las bromas, los sueños compartidos, las lecciones, los abrazos, el cariño, las charlas de café, las palabras de aliento, las correcciones, los abrazos, los silencios solidarios, la confianza, las ausencias inesperadas y las presencias sorpresivas.

Agradezco a la Universidad Nacional Autónoma de México por la formación humanista, por la oportunidad de crecer y aprender en sus aulas.

Agradezco a la Facultad de Ciencias Políticas y Sociales. A los profesores que fueron más allá de la academia y compartieron su experiencia personal y profesional.

A la Dirección General de Divulgación de la Ciencia por permitirme conocer la comunicación de la ciencia y la tecnología. Al equipo de Internet (Mónica, Ximena, Leo y Antonio) por el compañerismo y la amistad.

A mi asesora Lilia Ramos por disponer de su tiempo y experiencia para sacar este proyecto adelante.

A los sinodales Armando Rojas, Jacqueline Sánchez, Esperanza Cabrera y Nelly Becerril, por las observaciones que enriquecieron este trabajo.

Un agradecimiento especial al Maestro en Computación Roberto Sánchez Soledad, quien contribuyó al esclarecimiento del tema.

Por mi raza hablará el espírit

ÍNDICE

Introducción

El uso de Internet es cada vez más común. La cifra de usuarios se incrementa exponencialmente, al cierre de este trabajo, el último dato encontrado indica que son cerca de 30.6 millones de usuarios en México, cifra que tiende al crecimiento porque se trata de una herramienta que se inserta en la cultura de las nuevas generaciones. La tasa de crecimiento anual promedio es del 16 por ciento aproximadamente. Actualmente, quien no utilice Internet realmente está muy desactualizado. A pesar de los datos que parecieran alentadores, México se encuentra muy por debajo de países como Colombia, Chipre, Chile, Estados Unidos, etc., en cuanto al acceso a Internet.

Un hecho innegable es que el uso de Internet es cada vez más frecuente. El crecimiento de los usuarios de este medio es exponencial y los hábitos de los internautas se han diversificado en función de la oferta y las posibilidades que ofrece Internet. Ahora no sólo se accede a páginas personales, de consulta y búsqueda; también se pueden realizar operaciones bancarias, compras y transacciones.

Desde la aparición de la red Internet hasta la fecha hay un aspecto que continúa en desarrollo: la seguridad. Aunque en un principio fue un aspecto secundario frente al diseño de equipos que fueran más pequeños y portables, hoy en día es un tema de prioridad. Esto gracias a que la cantidad de información confidencial que se transmite a través de la red, es cada vez mayor. Pero así como se han desarrollado las modalidades para vulnerar los sistemas, también se han desarrollado algunos recursos que hacen logran una navegación segura.

No obstante, la confianza en el nuevo medio aún no es total. Esto se debe, principalmente, al desconocimiento que tenemos del mismo y es aquí donde el

reportaje adquiere relevancia, pues aporta elementos que permiten al usuario generar entornos confiables para realizar operaciones bancarias o compras.

La seguridad en Internet es un tema de interés general, una preocupación, y ésta se incrementa si hablamos de aspectos como los ya mencionados. La confidencialidad de la información que se trasmite por este medio, es un aspecto de vital importancia, pues se trata de datos que podrían ser utilizados para perjudicarnos. Sin ánimo de alarmar, pero sí de alertar a los usuarios.

Aunado a esto tenemos que promover la cultura en Seguridad, difundiendo las buenas prácticas de seguridad que nos llevarán, finalmente, a tener una mayor confianza al momento de la navegación. Es aquí donde el periodismo puede, y debe, intervenir para la difusión de dichas prácticas. El reportaje es uno de los géneros periodísticos considerado el más completo; una de las razones es que permite ver un tema en su conjunto, con cada una de las aristas que lo conforman. En el reportaje se explican los elementos y se establecen las relaciones entre ellos. En este género periodístico no sólo se informa, también se explica y, en ocasiones, se analiza.

Otra razón que convierte al reportaje en, lo que algunos llaman, “el rey de los géneros”, es la posibilidad que tiene el periodista para abarcar diversos géneros periodísticos. Esto, sin duda, es una gran ayuda y enriquece la investigación, pues amplía el abanico de herramientas de las cuales se puede auxiliar el reportero.

Al ser más explicativo, el reportaje permite despejar una mayor cantidad de dudas respecto a temas que, por su naturaleza, es difícil explicar. Es decir, temas como el abordado en este reportaje: la seguridad informática, o bien, otros que tienen una gran carga técnica para un lector promedio, pueden ser explicados con mucho mayor detalle.

En este aspecto, se abordó la seguridad en Internet desde dos puntos de vista que son relevantes por sus implicaciones sociales: el aspecto legal, es decir, qué leyes

nos protegen en caso que seamos víctimas de un fraude, por ejemplo, con qué herramientas legales contamos tanto como usuarios promedio como empresas; en cuanto al aspecto técnico, no se abundó demasiado, considerando que no se trata de un texto dirigido para expertos escrito por expertos; en este sentido se trató de aportar algunos elementos básicos de las buenas prácticas de seguridad para los usuarios, a fin de aportar un grano de arena a la conformación de una cultura en seguridad.

El tema se eligió porque uno de los objetivos que se persigue en el periodismo es que se traten temas de actualidad y de interés social, requisitos que cumple. Aunque el interés estaba enfocado en los sitios de instituciones bancarias, en el transcurso de la investigación también se trató un tema que tiene que ver con las transferencias electrónicas: el comercio electrónico.

Internet puede ser un gran aliado, una herramienta, pero hay que tomar en cuenta que la seguridad debe ser una prioridad. Primero hay que conocer cómo utilizarlo, el marco jurídico que nos respalda y los elementos técnicos que nos permiten tener un entorno seguro como usuarios. Hoy en día, hay muchas formas de procurar tener estos entornos de seguridad. Desde un elemento tan fundamental como puede ser la instalación y actualización de un antivirus, el desarrollo de contraseñas efectivas y seguras; hasta el poder identificar los sitios seguros de los que no lo son. Medidas sencillas pueden generar un ambiente seguro.

A la par del desarrollo de la seguridad en Internet también han evolucionado las modalidades de delitos en la red como los fraudes, suplantación de identidad, modificación de información, destrucción de información, entre otras. Es por ello que considero que no es un tema del todo agotado, además veremos cómo se desarrollan las nuevas tecnologías y, por ende, los intentos por transgredir la seguridad.

Para abordar un tema tan complejo, iniciamos en el Capítulo I con la seguridad de la red desde un punto de vista general, el respaldo que como sociedad tenemos desde el Estado y los organismos internacionales, considerando que este medio desconoce las fronteras geográficas. Se explica la dificultad que representa tratar de regular este medio a nivel internacional.

También se menciona que sí ha sido posible trabajar con las recomendaciones internacionales, que son estándares al momento de elaborar las normatividades de cada país. Además hay organizaciones como la Asociación Mexicana de Internet, que trabajan con organizaciones de otros países a fin de mantener un vínculo en materia de seguridad.

Hay una legislación que está vigente en nuestro país pero que se ha tenido que adecuar para dar cobertura a aspectos como la seguridad en Internet y la protección de los usuarios. Es así que en diferentes leyes se han hecho modificaciones para adecuarlas. Sin embargo, aún se estudia la posibilidad de establecer una ley específica para este medio.

Se realiza una revisión de la definición de hackers, pues se les ha considerado durante mucho tiempo como los responsables de los ataques a los sistemas informáticos. Como veremos, no todos se dedican a esto con fines maliciosos, ni se les puede encasillar como delincuentes, pues sus objetivos están definidos. Incluso han conformado comunidades que delinean conductas éticas de estos desarrolladores.

En el Capítulo II se trata el tema, de manera más específica, de la banca electrónica. Los elementos que constituyen a los portales bancarios en el aspecto de la seguridad, las medidas que han tomado en función de las experiencias pues, como todo nuevo medio, Internet y la seguridad se construyen en la marcha. Aunque no se

habla de experiencias particulares, sí hay estándares en la manera que tienen las instituciones bancarias al momento de proteger la información de los usuarios.
También se revisan otros servicios que han servido para incrementar los niveles de seguridad al momento de realizar transacciones bancarias como el Sistema de Pagos Electrónicos Interbancarios (SPEI). Este sistema es un intermediario y verificador de las operaciones entre instituciones bancarias. Se trata de una iniciativa desde la Secretaría de Hacienda y Crédito Público para evitar que se realicen transacciones sin autorización de los cuentahabientes.

El Comercio Electrónico forma parte también de este apartado, la razón principal es por que comparten algunos puntos, ambos: utilizan información confidencial de los usuarios para poder operar, requieren de uno o varios sistemas de verificación, utilizan sistemas de protección de datos similares. Además, para realizar compras por Internet el sitio tiene que constatar la información del usuario que desea realizar la operación con la institución bancaria; asimismo, el instrumento de pago en Internet es la tarjeta bancaria (crédito o débito).

Finalmente, en el Capítulo III se aborda el aspecto de la seguridad desde el usuario. Se establece que una pieza fundamental en el ámbito de la seguridad es el cuentahabiente. Al momento de realizar una operación bancaria, no sólo se debe responsabilidad a la institución que proporciona el servicio; el usuario es el que debe generar su propio entorno confiable. En este punto, le damos medidas fundamentales para generar un ambiente de seguridad.

La banca en línea es una alternativa que puede ser muy funcional en el ahorro de tiempo, costos, recursos, pensemos en la cantidad de papel que se ahorraría, si todos consultáramos nuestro estado de cuenta por Internet. Para evitar que se convierta en un entorno inseguro, es preciso educar al usuario para que utilice dichos servicios reduciendo al máximo posible los riesgos que se corren en un entorno abierto como Internet.

CAPÍTULO I

LA SEGURIDAD EN INTERNET. UNA PREOCUPACIÓN LATENTE.

Imagine que un día se levanta y decide consultar su estado de cuenta a través de Internet. El banco le ofreció este servicio que le ahorra tiempo y esfuerzo. Al ingresar al portal introduce el número de cuenta y su *password*. Pero al revisar su cuenta descubre que tiene un depósito por 100 mil pesos, usted asombrado no da crédito a semejante hecho y piensa que se puede tratar de un error de la institución bancaria, o bien, que fue acreedor a un premio por ser un cliente con cierta trayectoria bancaria. Decide averiguar qué ocurre, pero tiene algo importante que hacer y lo deja para después. Ya llamará luego. En la tarde vuelve a revisar su estado de cuenta y para su sorpresa tiene un retiro por 100 mil pesos. Su cuenta ha sido utilizada por alguien más.

En los últimos años el número de internautas se ha incrementado exponencialmente pero también las modalidades de delitos en línea. De acuerdo con el más reciente estudio presentado por la Asociación Mexicana de Internet en México hay cerca de 30.6 millones de internautas[1]. El crecimiento se ha registrado desde el 2005, cuando habían 17.2 millones de usuarios; luego para el 2006 la cifra incrementó a 20.2 millones; en el 2007 ya eran 23.9 millones de usuarios; y en el 2008, 27.6 millones, es decir, tan sólo del 2007 al 2008 la tasa anual de crecimiento de internautas fue del 16.4%[2].

[1] Verónica Valencia, "Crece internautas 11% desde 2008", [en línea], Distrito Federal, Reforma.com, 17 de mayo de 2010, Dirección URL: http://www.reforma.com/interfase/articulo/555/1109131/ [Consulta 17 de mayo de 2010].
[2] Estudio AMIPCI, *Hábitos de los Usuarios de los usuarios de Internet en México: Resumen Ejecutivo,* [En línea], México, Asociación Mexicana de Internet, Mayo 2009, Dirección URL: http://www.amipci.org.mx/estudios/temp/RESUMENEJECUTIVOEstudioAMIPCI2009UsuariosdeinternetFINAL-033472500124569126OOB.pdf, [Consulta: 10 de mayo de 2010].

No obstante que este crecimiento pareciera alentador, si lo comparamos con lo que ocurre en otras partes del mundo veríamos que a nuestro país aún le falta un tramo importante para estar a la vanguardia. Si observamos los resultados arrojados por el reporte realizado por el World Internet Project, México está dentro de los países con los porcentajes más bajos de usuarios de Internet con apenas el 32 por ciento, se encuentra por debajo de Portugal (37 por ciento), Chipre y Colombia (45 por ciento), República Checa (51 por ciento) y Chile (55 por ciento). En cuanto a los primeros lugares se encuentran: Estados Unidos (78 por ciento) y Chile (55 por ciento)[3]. Lo anterior refuerza la idea de que Internet no ha llegado a todos los sectores, ni a todas las personas, sin embargo, ya forma parte de la vida diaria de muchas.

Internet es parte fundamental de nuestras actividades, como lo expresa el maestro Roberto Sánchez Soledad, jefe del Área de Atención a Incidentes del CERT-UNAM:

> ¿Internet va a ser una herramienta para realizar transferencias?, creo que esa pregunta hubiera sido hace diez años, hoy en día el Internet es para eso literalmente. Hay empresarios, todo se maneja absolutamente por Internet. Entonces la persona que no utilice Internet hoy en día, si están muy desactualizada.
>
> Prácticamente las amas de casa usan Internet, es muy seguro, así como existen muchas formas de espantarnos, si así se puede decir, por todo lo que existe en Internet, llámese hackers, intrusos, lo que quieras, también existen muchas formas de protegernos, de poder navegar. Así como existen cuestiones que nos espantan, existen cuestiones que nos benefician[4].

Esta inserción de Internet ha sido favorable en términos de productividad, lo cual se puede ver reflejado en el tiempo de ejecución de algunas tareas; pero, paralelamente

[3] Justin Pierce, *World Internet Project Report finds large percentages of Non-users, and significant gendre disparities in going on line*, [on line, PDF], USC ANNENBERG School for Communication & Journalism, 26 de febrero de 2010, Dirección URL: http://www.worldinternetproject.net/ [Consulta: 28 de Mayo de 2010]

[4] Entrevista, 11 de octubre.

a esto, ha crecido la actividad delictiva en la red y otros actos que no son precisamente “delitos” sino infracciones civiles o administrativas. Por lo que las facilidades que ofrece Internet vienen acompañadas de una preocupación: la seguridad de la información. Como en los siguientes ejemplos:

El pasado 19 de febrero El País publicó la siguiente nota: “Una red roba datos clave de 74.000 ordenadores en el mundo”[5]. La historia era de una “red de cibercriminales”, que durante un año y medio, se había infiltrado en las computadoras de 100 mil usuarios, en 196 países, para robarles información de cuentas de correo electrónico, redes sociales, nombres de usuario, claves de acceso y preguntas de seguridad de portales web de banca online. En total se habían robado cerca de 75 *Gygabites* de información.

De acuerdo con NetWitness, una empresa estadounidense dedicada a la seguridad *online*, reveló que esta organización, cuyos miembros operaban desde China y Europa utilizaban una técnica conocida como *phishing* para infectar las computadoras con un troyano, conocido como *Kneber*. Funcionaba de la siguiente manera: El usuario recibía un mensaje en su correo electrónico con un enlace que aparentemente lo redireccionaba a la página principal de un banco, u otro portal conocido, con logos y demás mensajes que lo hacían más creíble.

Al darle *click* a estos mensajes, se descargaban paquetes de *software* infecciosos cuyo objetivo era burlar los programas de seguridad de la computadora. Una vez lograda la infección, el troyano entraba en acción y robaba la información enviándola a un servidor origen. Afortunadamente se detectó el origen de este fraude y se desmanteló la red.

[5]David Alandete, “Una red roba datos clave de 74.000 ordenadores en el mundo”, [en línea], España, El País.com, 19 de febrero de2010, Dirección URL: http://www.elpais.com/articulo/sociedad/red/roba/datos/clave/74000/ordenadores/mundo/elpepisoc/20100219elpepisoc_2/Tes [consulta: 14 de mayo de 2010]

La preocupación en el aspecto de la seguridad en Internet es creciente, pues así como evolucionan los antivirus y la protección, también incrementa las formas en las que se pueden cometer fraudes. En el caso de *Kneber*, por ejemplo, la principal preocupación era que menos del 10 por ciento de los antivirus existentes detectaba esa infección.

Los costos de este tipo de fraudes ascienden a miles. En otro caso similar, por ejemplo, se detuvo a siete personas que habían cometido un fraude por 45 mil 334 euros[6]. Estas personas utilizaron el *phishing* para obtener claves de usuarios de banca electrónica, una vez obtenida esta información ordenaban a las entidades bancarias realizar envíos de dinero a otras cuentas. En tan sólo 16 horas (entre el 12 y el 13 de noviembre del 2009) realizaron un total de 15 transferencias bancarias.

Ante el incremento del uso de Internet como medio para la realización de transacciones bancarias también crece la preocupación por la seguridad de la información. "La red Internet es una red pública, por lo que el riesgo de que las amenazas contra la autenticidad, integridad, confidencialidad y el no repudio de las transacciones que sobre ella se realicen será mayor"[7]. Al ser Internet una red pública y abierta, como señala Jordi Buch, se incrementa exponencialmente el riesgo.

Internet ha superado las fronteras geográficas y esa es otra preocupación. Pensemos en el caso de un grupo de 13 personas que fueron arrestadas por realizar transferencias electrónicas como intermediarios a cambio de una comisión. Este grupo simulaba actuar en nombre de empresas con diferente objeto social dedicadas, por ejemplo, a la compra-venta de maderas y diversas actividades

[6]Europa Press, "Detenidas siete personas por fraude mediante '*phishing*'", [en línea], España, El País.com, 8 de abril de 2010, Dirección URL: http://www.elpais.com/articulo/tecnologia/Detenidas/personas/fraude/mediante/phishing/elpeputec/20100408elpeputec_6/Tes, [Consulta: 14 de mayo de 2010]

[7] Jordi Buch i Tarrats y Francisco Jordan, *La Seguridad de las transacciones bancarias en Internet*", [en línea, PDF] Pamplona, Sociedad Española de Informática de la Salud, 2001. Dirección URL: http://www.conganat.org/seis/informes/2001/PDF/6BuchTarrats.pdf, [Consulta: 10 de mayo de 2010].

financieras. Estos actuaban como intermediarios y recibían dinero en sus cuentas y, a cambio de una comisión, enviaban el dinero a países como Ucrania, Moldavia o la República Checa[8].

La revolución que supone Internet, como lo plantea Santiago Muñoz Machado, "está afectando éste tan profundamente a la economía general y a los mercados del sector, se augura que transformará de modo tan señalado los hábitos de la vida ordinaria, la cultura, el ocio, el trabajo, la empresa, el ejercicio de las profesiones, la prestación de toda clase de servicios […] etcétera"[9]. Esta inserción a la vida cotidiana tiene que ir acompañada de otros elementos, pues si Internet supone una revolución en materia tecnológica también debe plantearse una modificación que nos garantice un entorno con todas las garantías de seguridad. Para ello es fundamental, como usuarios, tener algunos elementos que nos permitan entender cómo se maneja el ciberespacio y cómo nos pueden afectar a través de él.

Hay otro asunto relacionado con las transferencias electrónicas y la seguridad, se trata de cómo los grupos del crimen organizado utilizan estos medios. Se estima que cada año ingresan a México ente 19 mil y 29 mil millones de dólares desde Estados Unidos provenientes de actividades ilícitas, de acuerdo con el gobierno de ese país[10]. Mientras que la Secretaría de Hacienda y la Asociación de Bancos de México reconocieron que cada año hay un promedio de 10 mil millones de dólares con un origen poco claro[11].

---

[8] s/a, "14 detenidos por robar datos bancarios en Internet", [en línea], España, El País.com, 29 de junio de 2009, Dirección URL: http://www.elpais.com/articulo/sociedad/detenidos/robar/datos/bancarios/Internet/elpepusoc/20090629elpepusoc_4/Tes [Consulta: 14 de mayo de 2010].

[9] Santiago Muñoz Machado, *La regulación de la red: Poder y Derecho en Internet*, España, Ed Taurus, 2000, p 11.

[10] Tania M. Moreno. "Las 5 caras del lavado de dinero", [en línea], CNN Expansión, Ciudad de México, martes 08 de junio de 2010, Dirección URL: http://www.cnnexpansion.com/economia/2010/06/07/lavado-de-dinero-narco-mexico-eu [onsulta: 25 de octubre de 2010].

[11] Alberto Nájar. "Nuevas reglas contra el lavado de dinero en México", [en línea], BBC Mundo, México, última actualización: martes 15 de junio de 2010, Dirección URL:

En el Estudio Binacional de Bienes Ilícitos México-Estados Unidos, se plantea que las organizaciones criminales operan una compleja red de procesos para contrabandear bienes ilícitos desde EEUU, ya sea a través de transferencias electrónicas, efectivo o tarjetas de prepago[12]. Tal vez lo más grave del asunto es que algunas instituciones financieras se prestan para dicho fin, sin que haya detenidos al respecto:

> Algunos de los principales bancos y empresas financieras estadounidenses, entre ellos Wells Fargo, Bank of America, Citigroup, American Express y Western Union, han lucrado durante años con el lavado de fondos provenientes del narcotráfico y sólo pagan multas mínimas, sin que ningún ejecutivo sea encarcelado cuando las autoridades logran detectar el negocio ilícito. […]
>
> Todo esto se reveló en un acuerdo judicial del banco con fiscales federales, en marzo de 2010. En los documentos oficiales judiciales del caso, revisados por *La Jornada*, Wachovia admitió que no hizo lo suficiente para detectar fondos ilícitos en su manejo de más de 378.4 mil millones de dólares en sus negocios con casas de cambio mexicanas entre mayo de 2004 y mayo de 2007.
>
> De ese total, Wachovia procesó por lo menos 373.6 mil millones en transferencias electrónicas, más de 4.7 mil millones en traslados de efectivo, y otros 47 millones en depósitos de cheques internacionales. No todos estos fondos están vinculados con el narcotráfico, pero, según investigaciones del Departamento de Justicia, miles de millones no fueron sujetos a la vigilancia ordenada por la ley, y cientos de millones de dólares de estos fondos sí han sido ligados directamente con el narcotráfico[13].

En la Estrategia Nacional para la Prevención y el Combate al Lavado de Dinero y el Financiamiento al Terrorismo, presentada por el presidente Felipe Calderón Hinojosa, se plantea un monitoreo de los recursos, una de las estrategias es la limitación de la compra-venta de bienes con dólares en efectivo, que es una de las

---

http://www.bbc.co.uk/mundo/economia/2010/06/100615_2119_mexico_lavado_dolares_gz.shtml [Consulta: 06 de agosto de 2010]

[12] Tania M. Moreno, *ibid.*

[13] David Brooks, "Grandes bancos de EU aceptan lavar narcofondos mexicanos", [en línea], La Jornada On Line, México, 30 de junio de 2010, Dirección URL: http://www.jornada.unam.mx/2010/06/30/index.php?section=economia&article=025n1eco [Consulta: 20 de Septiembre de 2010]

modalidades del lavado de dinero. Sin embargo, no se observa una acción directa en las transferencias electrónicas, pero como ya observamos se trata de una importante modalidad en la transferencia de fondos, reconocido en el mismo documento presentado por el Presidente:

> Dependiendo del mecanismo que se emplee en la etapa de colocación de los recursos de procedencia ilícita, las organizaciones criminales llevan a cabo una serie de operaciones para ocultar su origen e impedir el rastreo de la fuente. Por ejemplo, en el caso de la introducción en instituciones financieras mexicanas de dólares derivados del narcotráfico, se han observado transferencias electrónicas de fondos a instituciones financieras en EEUU y Asia simulando, principalmente, transacciones de operaciones comerciales internacionales[14].

Algunos expertos coinciden en que estas nuevas reglas son necesarias pero insuficientes. Actualmente la banca en México cuenta con sistemas de cómputo y software que permite identificar la conducta de cada cliente y también cuando una persona moral o física sale del patrón habitual, como señaló la Asociación de Bancos de México[15]. No obstante aún contamos con algunos huecos sobre todo en materia legal.

¿QUÉ SON LOS DELITOS INFORMÁTICOS?

Los anteriores son sólo algunos ejemplos de los alcances de Internet en manos de algunas personas que aprovechan la red para fines no necesariamente correctos. ¿Pero qué es un delito informático? ¿Todo puede ser considerado como un "delito" cuando hablamos de información?

[14] Gobierno Federal, SEGOB, SHCP, SSP, PGR, *Estrategia Nacional para la Prevención y el Combate al Lavado de Dinero y el Financiamiento al Terrorismo*, Gobierno Federal, México, http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/814619//archivo [Consulta: 20 de septiembre de 2010].
[15] Tania M. Moreno, *ibid*.

Vamos a regresarnos un poco. El 17 de mayo de 1999, se incluyó en el contenido del Diario Oficial de la Federación una nueva figura jurídica: “Acceso ilícito a sistemas y equipo de informática”. Con esto la legislación mexicana se colocaba en uno de los principales países en prever esta figura dentro de su marco jurídico. “En dicha fecha, dos clases de público (tecnológico y jurídico) reciben una reforma integral en materia penal, misma que se orienta principalmente a dos temas específicos: la protección de la propiedad intelectual así como la protección de los usuarios de las tecnologías de información”[16].

En tan sólo 10 años se dio un avance muy importante, como señala Ivonne Muñoz Torres, la legislación de casi todos los estados de la República ahora tienen contemplada esta figura en su marco jurídico, siendo que en un principio sólo el estado de Sinaloa lo consideraba. Ivonne Muñoz Torres, abogada especialista en Tecnologías de Información y Comunicación nos señala:

> El punto de partida para discernir con claridad el tema de los “Delitos Informáticos”, es dejar claro que no todas las acciones que no son aceptables por la sociedad son “Delitos”. El Derecho reconoce otras figuras jurídicas a través de las cuales se cometen actos antijurídicos, en su caso se les denomina infracciones civiles o administrativas; para el tema de las Tecnologías de la Información, existen algunas acciones que se encuadran bajo este tipo de figura y no meramente bajo el concepto de delito[17].

Por ahora nos ocuparemos de aclarar algunos conceptos. La misma autora nos señala que hay una gran variedad de términos que pueden llegar a usarse refiriéndose a lo mismo, pero es menester señalar que no todo se aplica a todos los casos, sobre todo cuando se trata de castigar ciertas conductas antijurídicas, es necesario aclarar conceptos. Entre los que llegan a utilizarse para referirse a los delitos que se cometen a través de Internet tenemos: Delitos cibernéticos, delitos electrónicos, delitos computacionales, delitos telemáticos, y delitos informáticos. No

[16] Ivonne Muñoz Torres, *Delitos informáticos: Diez años después*, México, Ed Ubijus, 2009, pág. 1.
[17] *Ibid,* p.13.

nos detendremos demasiado en aclarar todos los conceptos pero sí retomaremos los conceptos aportados por la jurista, pues son lo bastante claros al respecto:

- **Delitos cibernéticos**: "es aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar las comunicaciones que se llevan a cabo a través de las Tecnologías de Información y Comunicación. Un ejemplo: ataque de denegación de servicio, mejor conocido como *Denial of service*"[18].

- **Delitos electrónicos**: "es aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar el flujo electrónico de datos, y que en consecuencia afecte el funcionamiento de Internet así como de los Sistemas de Información que dependen de la electrónica para desarrollarse. Por ejemplo: ataque a las instalaciones físicas de las cuales dependa una red pública de telecomunicaciones"[19].

- **Delitos computacionales**: "se define como aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar las operaciones de una computadora y cuya consecuencia sea la interrupción de cualquiera de las fases de procesamiento de datos"[20]. Por ejemplo: La modificación de los comandos u órdenes en las cuales se basa la operación de un sistema.

- **Delitos telemáticos**: "se define como aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar las telecomunicaciones y/o las tecnologías de información, cuya consecuencia

[18] Ivonne Muñoz Torres, *ibid* p.15.
[19] *Ibid.*
[20] *Ibid,* p.16.

sea la interrupción de la transmisión de información que esté depositada en un sistema de información. Un ejemplo: Interrupción de comunicaciones"[21].

- **Delitos Informáticos**: "Con la conjunción de estos tres conceptos: informática, información y datos, es entonces como se debería crear la definición de delito informático, mismo que se define como aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar datos, información o sistemas de información cuya consecuencia sea el daño directo o indirecto en ellos así como el mal uso de éstos"[22].

Entonces, aunque todos estos conceptos se relacionan de una u otra manera, no pueden ser utilizados indistintamente como vemos en su propia definición. Por ahora, nos quedaremos con el concepto de Delitos Informáticos por ser el que se refiere mejor al tema que nosotros estamos tratando. Como Ivonne Muñoz también explica todos estos delitos están previstos en el marco jurídico vigente. Incluso las legislaciones de casi toda la República Mexicana contemplan sanciones para los infractores.

Uno de los principales problemas al momento de regular el ciberespacio en materia legal radica en que Internet no está delimitado dentro de los márgenes de una jurisdicción. Un delito puede cometerse desde diferentes partes del mundo y esto dificulta la persecución y castigo, pues además cada país cuenta con una normatividad distinta. Pero lo que sí se ha logrado son acuerdos internacionales que permiten una estandarización conceptual y, por ende, que esta pueda ser tomada por todos los países.

Como usuarios de la banca electrónica, de la cual profundizaremos más adelante, adelantaremos que entre los ataques[23] más frecuentes están:

[21] Ivonne Muñoz Torres, *ibid,* p.17.
[22] *Ibid,* p.18.
[23] Jordi Buch i Tarrats, *ibid.*

~ **Robo de información:** Es la obtención de información mediante escuchas de red. Entre la información que más se busca están: los números de cuentas o de tarjetas de crédito, balances o información de facturación. Estos ataques permiten el robo de servicios normalmente limitados a suscriptores de servicios.

~ **Saturación de correo SPAM:** Es el envío masivo de correos electrónicos. Estos correos pueden llegar a ser un verdadero fastidio para los usuarios, pues pueden saturar su buzón, pero también pueden ir cargados con paquetes de software malicioso que se descarga en automático, generando una infección en su computadora.

~ **Suplantación de identidad:** Este permite al atacante realizar operaciones con la identidad de otro usuario, sin autorización. Una situación de este tipo permitiría a un poseedor de miles de números de tarjetas de crédito la realización de pequeñas operaciones aparentemente insignificantes, pero que en suma pueden llegar a cifras millonarias. También puede interesar al atacante la suplantación de identidad del usuario de banca virtual.

~ ***Sniffers*:** Son herramientas informáticas que permiten obtener lecturas de la información que se transmite por la red como *passwords* o información de operaciones. Los *sniffers* permitirían la consumación de un ataque de suplantación de identidad y/o robo de información.

~ **Modificación de información:** Este tipo de ataque permite alterar el contenido de transacciones como pagos, cantidades o incluso la propia orden de compra. Es decir, permite modificar la información de facturación o de una transacción.

- **Repudio:** Es el rechazo o negación de una operación por una de las partes, esto puede ser problemático para los sistemas de pago. Si una de las dos partes rechaza un previo acuerdo, ésta deberá soportar costos adicionales de facturación.

- **Denegación del servicio:** En este caso se inhabilita al sistema para que pueda operar normalmente, por lo tanto imposibilita la realización de operaciones transaccionales. Éstos son de extrema sencillez y la identificación del atacante puede llegar a ser imposible.

Como podemos observar, un sistema puede ser vulnerado de distintas maneras, sin embargo, el conocimiento de estos ataques y las medidas que pueden seguir los usuarios, son la mejor defensa para evitar algún ataque, como veremos más adelante.

La tecnología avanza a pasos acelerados, por lo que las modalidades para vulnerar un sistema también evolucionan. Por ello debemos aclarar que aquí sólo se mencionan algunas formas en las que se pueden atacar la seguridad y que las posibilidades no se agotan aquí. Asimismo las definiciones también se modificarán con el tiempo, pues no es un tema que esté agotado por completo.

***HACKERS*. ¿QUIÉNES SON?**

Al momento de pensar en los *hackers* podría remitirnos a una definición negativa, vincularlos directamente con la delincuencia, la infiltración, el robo de información, es decir, con todo aquello que atente contra la seguridad de la información o de los sistemas. Esta palabra podría remitirnos, incluso, al peligro en Internet.

Tal vez se deba al origen del término y a la fama que ha adquirido gracias a los medios de comunicación. El caso es que en este momento de la historia ya hay una

definición más clara de lo que son los *hackers* y los objetivos que persiguen, incluso hay una lucha constante de algunos para dejar claro las finalidades de cada tipo de *hacker*.

Si le pidieran una definición de *hacker*, ¿cuál sería su respuesta?, tal vez le vendría a la mente la imagen de una persona que vive pegada a una computadora, buscando la manera de ingresar a otros sistemas, ¿para qué?, para obtener la satisfacción de saber que tiene el conocimiento y la habilidad para hacerlo; probablemente, crea, que es una cuestión de orgullo y satisfacción personal; quizá para obtener algún beneficio económico.

Este dibujo del *hacker* no es del todo preciso. Sin embargo, conocer y definir a estos personajes informáticos es un reto, pues la mayoría mantiene su identidad anónima y se identifican con seudónimos. Hay comunidades virtuales en las que se generan algunos debates por distinguir a los que se dedican a identificar las debilidades de los sistemas para reforzarlos, de los que se dedican a actividades ilícitas. Algunos expertos en seguridad como Marcus J. Ranum coinciden en que el *hacking* tiene variantes:

> El *Hacking* (acceso no autorizado a sistemas informáticos) es un fenómeno excitante y a veces temido, dependiendo del lado de la fortaleza en que usted se encuentre. [...] A un lado de la fortaleza, en el interior, se encuentran los frustrados administradores de la red y los profesionales de la seguridad que son responsables de la construcción y del mantenimiento del, cada vez más importante, tejido cibernético de la vida actual. Al otro lado de la fortaleza se encuentra una variada horda de *hackers*, que disfrutan descubriendo las grietas existentes en los muros y dando publicidad periódica a los agujeros que hay en las defensas de, incluso, los más importantes y los más poderosos[24].

Hay quien identifica a los *hackers* como parte de una comunidad *underground*, o una subcultura. La historia de cómo nace el término *hacker* se remite a los años 70's,

[24] Stuart McClure, Joel Scambray y George Kurtz, *Hackers: Secretos y soluciones para la seguridad de redes*, España, Osborne McGraw Hill, Biblioteca Profesional, 2000, p. xxiii.

cuando “un estudiante de ingeniería electrónica llamado John Draper encontró una forma de vulnerar el sistema telefónico y hacer llamadas sin pagar”[25].

La fama que adquirió John Draper inspiró a un grupo importante de aficionados a la tecnología telefónica, crearon comunidades en las que compartían conocimientos. Para cuando las compañías telefónicas y el gobierno se dieron cuenta, ya había un grupo, los famosos *phreaker*, quienes conocen y manipulan los sistemas telefónicos[26].

“El Capitán Crunch siempre alegó que su acciones sólo estaban motivadas por el deseo de aprender acerca del sistema telefónico”[27]. Es justamente el reto intelectual de conocer un sistema profundamente lo que motiva a las personas que incursionan en este mundo. Como es el caso de los *hackers*, que ya estaban presentes desde los años 60’s, y eran individuos con un profundo conocimiento en sistemas, los cuales manipulaban[28].

La aparición de las computadoras personales en los 70’s supone una verdadera revolución tecnológica y su origen se remonta a las comunidades de jóvenes entusiastas que encontraban estimulante la idea de tener una computadora en casa (cabe destacar que antes de esto, las computadoras sólo estaban en poder de universidades, bancos y el gobierno, por el costo y el tamaño).

En el mismo periodo se gestó otro movimiento que hoy en día es fundamental: *software* libre, en el cual se defiende el total y libre acceso a los programas informáticos. El principio es que el código fuente esté abierto y libre de candados, para que otras personas puedan modificarlo.

---

[25] Ximena Gutiérrez Velázquez, “Los *hackers*: en los límites de lo posible”, Revista ¿cómo ves?, Año 12, Núm. 138, México, UNAM/DGDC, mayo, 2010, pág 16.
[26] *Ibid.*
[27] *Ibid.*
[28] *Ibid,* p.17.

Este movimiento derivó en una serie de aplicaciones que hoy en día están disponibles a muchas personas, algunas gratuitas y otras no. Cabe precisar que "libre" no es igual que "gratuito", pero la gran ventaja es que todos estos desarrollos son accesibles para que puedan ser mejorados y/o modificados.

Regresando al movimiento *hacking*, intentar infiltrarse en una red puede tener varios objetivos, por ejemplo, para detectar sus debilidades y corregirlas, al menos para eso algunos *hackers* son contratados por empresas. Un *hacker* conoce el sistema e intenta infiltrarse, pero la finalidad no es necesariamente el robo de información o el fraude. Es aquí cuando vale precisar que hay diferentes tipos de *hackers*, clasificación que surgió, precisamente, para distinguir entre los que se dedican a mejorar la seguridad.

De manera genérica, durante mucho tiempo, *hacker* definía a todos aquellos individuos que se infiltraban en los sistemas informáticos, como ya hemos explicado. No obstante hoy la comunidad de *hackers* se han esforzado por precisar quién es quién en el mundo del *hacking*. Es así como tenemos los siguientes tipos:

- ***Black Hat Hacker*** **("sombrero negro") o *crakers*:** Son aquellos que sin autorización y con intenciones maliciosas "violan sistemas informáticos para robar o modificar la información. Se les asocia también con ataques de virus, *spam* y gusanos"[29].

- ***White Hat Hacker*** **("sombrero blanco"):** Es aquel que se infiltra a los sistemas y realiza ataques con el fin de probarlos, el objetivo de estos individuos es encontrar debilidades y mejorar la seguridad de los mismos, cuentan con autorización pues, generalmente, los contratan para dicho fin.

[29] Ximena Gutiérrez Velázquez, *Ibid* p.18.

A las empresas, organizaciones e instituciones les resulta rentable contratar a estos individuos para evitar la infiltración y robo de la información. Cuando una empresa detecta que se ha vulnerado la seguridad de sus sistemas y se detecta el origen del ataque pueden ocurrir dos cosas: una, que se detenga al sujeto; y la otra, que se le ofrezca un empleo.

- ***Grey Hat* ("sombrero gris"):** "Es el *hacker* que penetra sin autorización en sistemas informáticos, quizá sin propósitos maliciosos, pero que no necesariamente alerta a los administradores del sistema para reparar la falla"[30].

Como podemos darnos cuenta, no todos los *hackers* son maliciosos, incluso podemos hablar de códigos de ética. No todas las motivaciones son necesariamente robar información como las modalidades del *pharming* o el *phishing*, que se explicarán más adelante. El reto intelectual puede ser una gran motivación.

Otra muestra de que no todos se dedican a actividades maliciosas es que hoy en día existe una comunidad organizada, con una serie de actividades que van desde congresos hasta publicaciones, en donde difunden información de interés para la comunidad. Finalmente, esta palabra puede ir más allá de la primera impresión.

Richard Stallman, principal promotor del movimiento de software libre, identifica al *hacker* con un espíritu juguetón, ingenioso, que explora los límites[31]. A esta definición podemos agregar que es gracias a estos espíritus exploradores que hemos logado avances, desarrollos, mejoras, en el ámbito científico y tecnológico.

[30] Ximena Gutiérrez Velázquez, *Ibid, p.18.*
[31] *Ibid* p.19.

EL CIBERESPACIO Y LA LEY

Algunos organismos internacionales como la UNESCO, si bien no tienen la facultad para generar leyes en torno al tema de Internet y más específicamente a la seguridad, ni tienen la facultad para perseguir delitos, han realizado algunas aportaciones en cuanto a las consideraciones que deben tomar en cuenta los países al momento de generar leyes en esta materia.

Se podría decir, entonces, que no podemos hablar de una regulación internacional o una ley internacional para los delitos informáticos, sin embargo, se han tratado de establecer parámetros que funcionen como estándares para las legislaciones de cada país. Lo cual es necesario considerando las características de Internet como el hecho de que no tiene una delimitación geográfica y el constante desarrollo de la tecnología que abre las posibilidades de nuevas formas de cometer ilícitos.

En entrevista, el maestro Roberto Sánchez Soledad, Jefe del área "Atención a incidentes" de la Subdirección de Seguridad de la Información / UNAM-CERT habló acerca de la colaboración internacional en materia de Seguridad Informática:

> Hablar de una ley general para Internet es muy difícil, porque los ataques son diferentes. Cada día sale uno diferente. El problema de Internet es que estamos globalizados, entonces, si tú te vas a Timbuktu, desde allá puedes lanzar un ataque, un robo de información. Entonces la integración con todos los países es muy difícil.
>
> Se está dando foros de colaboración como FIRST, o Antiphishing Group. En estos foros se coordinan entre los CERT de diferentes países para atender los problemas comunes en cuanto a ataques, el hacerlo de otra manera toma tiempo y el tiempo en cuestiones informáticas va muy rápido esto. Nos gana.
>
> Por ejemplo tú quieres un acuerdo de colaboración por un delito informático a nivel internacional y no existe nada legislado. Primero que nada tienes que poner de acuerdo a las personas de otro país para que quieran generar un acuerdo de

> colaboración. Suponiendo que logras convencerlas, el siguiente punto vas a la Cámara de Diputados, a la Cámara de Senadores, metes la propuesta… ¿cuánto tiempo va a pasar para que esa propuesta pase?, un año, dos años, y si tú quieres resolver esto en un mes?
>
> Lo más seguro es que en ese tiempo ya se generaron nuevos ataques que no tenías contemplados en tu plan original. Por eso es que a veces el trabajo en foros es más efectivo, los acuerdos de colaboración interinstitucionales son más rápidos, sólo requiere de ponerse de acuerdo y realizarlo. Uno de los métodos que ya está comprobado [en acuerdos internacionales] es trabajar a través de los CERTS. Son cientos de CERT a nivel mundial y trabajar con ellos ha sido bastante bueno[32].

Si hablamos de la parte legal, Ivonne Muñoz plantea que se puede realizar una clasificación de los delitos informáticos en función de lo que el interesado quiere proteger. El objetivo de las leyes, los reglamentos, del marco jurídico en general, es "evitarnos un daño, ya sea de carácter personal, laboral o patrimonial"[33]. La misma autora plantea que algunas de las preocupaciones en el tema en el sector de las tecnologías de la información son, desde el punto de vista de las personas:

- Estados financieros y patrimoniales.
- Ingresos.
- Configuración de equipos personales.
- Invenciones marcas y obras.
- Documentos de trabajo (archivos históricos y correos electrónicos).
- Cartera de clientes.
- Ventas.
- Planes de negocio.
- Proveedores.

[32] Roberto Sánchez Soledad, entrevista, 11 de octubre de 2010.
[33] Ivonne Muñoz Torres, *Op. Cit. p.*23.

Pero como señalábamos no todo los actos pueden ser considerados como delitos. También se encuentran las infracciones civiles o administrativas, las cuales se encuentran previstas en otras normatividades. En el caso de México, los avances en materia de legislación han sido más o menos recientes, pero lo cierto es que se ha procurado atender esta problemática de la seguridad.

Hablando de banca virtual encontramos los siguientes delitos como los más comunes:

- Robo de información.
- Suplantación de identidad.
- *Sniffers*.
- Modificación de información.
- Repudio.
- Denegación del servicio.

¿Qué tipo de delitos electrónicos son considerados por la legislación mexicana?

Nuestra legislación cuenta con las sanciones para diferentes tipos de ilícitos, aunque no exista una ley específica que las englobe a todas. A continuación se presentan una serie de leyes en lo que se considera la comisión de delitos electrónicos.

1) **Ley Federal contra la Delincuencia Organizada**: operaciones con recursos de procedencia ilícita, la corrupción de personas, la pornografía de personas.

2) **Ley de Instituciones de Crédito**: Clonación de instrumentos de crédito y pago/*skimming*, utilización de instrumentos de crédito o pago falsificados, acceso ilícito a equipos y medios electrónicos del Sistema Bancario, utilización ilícita de recursos o valores, destrucción de información crediticia.

3) **Ley General de Títulos y Operaciones de Crédito**: Clonación de tarjetas de crédito, débito y de afinidad/*skimming*; utilización de instrumentos de crédito, débito y afinidad falsificados, acceso ilícito a equipos y medios electrónicos del Sistema Bancario.

4) **Ley del Mercado de Valores**: Destrucción de información financiera, la revelación o transmisión de información, sustracción o utilización de claves de acceso.

5) **Ley de la Propiedad Intelectual**: Reincidencia en la comisión de infracciones administrativas como el utilizar sin consentimiento del titular una marca registrada; revelación de secretos industriales, robo y uso ilegítimo de secretos industriales, robo y uso ilegítimo de secretos industriales por terceros no autorizados.

SEGURO EL CIBERESPACIO

No basta con entender que hay una legislación que castigue ciertas actividades delictivas, incluso saber que nuestro país considera el castigo para quien delinque a través de una computadora, puede darnos seguridad. Pero hay que entender qué tipo de actividades se llevan a cabo en la red y distinguir entre las que son “delitos” y las que son “faltas administrativas”.

Además de resolver algunos puntos que hacen de la regulación de Internet una labor difícil de resolver, sobre todo por su propia definición, según el diccionario de la Real Academia de la Lengua Española se define como: “La red informática mundial,

descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación"[34].

Cuando se diseñó Internet, parte de la seguridad se delegó a la idea del mutuo respeto y honor de los usuarios, así como al conocimiento de un código de conducta considerado "apropiado" en la red. Así que en principio se consideraba que sólo era necesario un mínimo de protección, esto es, un *login* y un *password*, pues se confiaba en la conducta ética de los usuarios, recordemos que Internet en sus orígenes era utilizado con fines militares y académicos.

No obstante: "la red Internet tiene problemas de autenticidad, integridad, confidencialidad y repudio afectando a los requerimientos de las transacciones electrónicas u operaciones de banca virtual"[35] como lo describe Jordi Buch i Tarrats y Francisco Jordan, en *La Seguridad de las transacciones bancarias en Internet*.

Una de las dificultades de tratar de regular este medio consiste en que se trata de un medio abierto, "una red mundial", incluso podríamos decir que se trata de un universo de información alterno, por lo que algunos legalistas han propuesto que se regule esta red mediante convenios internacionales estándar.

Actualmente se han tratado de establecer, mediante los organismos internacionales ya existentes como la Organización para la Cooperación y el Desarrollo Económico (OCDE), algunas normas o estándares en materia de seguridad en Internet, por ejemplo, en las cuestiones de comercio electrónico.

No es de extrañar que los usuarios aún tengan desconfianza en realizar algunas operaciones, sobre todo en lo que refiere a actividades financieras, considerando

[34] s/a, s/t, [online], España, Real Academia Española, Ed Espasa Calpe, 2008, 23.ª edición, Dirección URL: http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=internet, [Consulta: 5 de mayo de 2010]
[35] Jordi Buch i Tarrats, *ibid.*

que aún no se puede hablar de una red 100 por ciento segura, como lo refleja el *World Internet Project*, en donde se muestra que el 78 por ciento[36] de los usuarios de Internet no utilizan este medio para realizar compras.

Una de las posibles razones es por las preocupaciones con respecto a la seguridad, en donde México, de acuerdo con este mismo estudio refleja que el 53 por cierto de los encuestados está preocupados o extremadamente preocupados acerca de la seguridad de la información contenida en las tarjetas de crédito, que son datos que se proporcionan al momento de adquirir un producto vía Internet.

LA POLICÍA CIBERNÉTICA

Aunque el 17 de mayo de 1999, México logró un gran avance al agregar la figura jurídica de: "Acceso ilícito a sistemas y equipo de informática", que buscaba la protección de la propiedad intelectual así como de los usuarios de las Tecnologías de información, como ya mencionamos anteriormente.

Fue hasta el 11 de diciembre de 2002, cuando se creó el Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos (GCICDC). Coordinado por el Área de Inteligencia de la Secretaría de Seguridad Pública (SSP), éste fue el paso definitivo para la investigación y persecución de los delitos cometidos en Internet.

Este grupo, conformado por instancias del Gobierno Federal, prestadores de servicios e instituciones de educación superior, como la Universidad Nacional Autónoma de México, se conformó "con la misión de concentrar la información para identificar, monitorear, rastrear y localizar delitos como fraudes, falsificaciones, intrusión en sistemas de cómputo, explotación sexual comercial, pornografía infantil,

[36] Justin Pierce, *ibid.*

amenazas y todo ilícito que ocurra en Internet o se apoye en sistemas computacionales"[37].

Dicho grupo se creó considerando la vulnerabilidad que aún guarda el flujo de información en Internet, la cual es capitalizada por *hackers* y organizaciones criminales. Ya hemos tratado el tema de los *hackers,* es importante recordar que *hacker* no es sinónimo de criminalidad y que hay distinciones en la misma comunidad que se hacen en función de sus objetivos e intenciones.

Uno de los principales temas a los que se ha enfocado el GCICDC (aunque no es el único), es la detección de páginas dedicadas a la pornografía infantil, al menos es lo que se ve reflejado en los informes presentados desde su creación: "al recibir denuncias de páginas con pornografía infantil procedió a su destrucción inmediata"[38].

Los integrantes del grupo DC México son:

→ Entidades del Poder Ejecutivo Federal, integrantes del gabinete de Seguridad Nacional.

→ El Poder Legislativo Federal a través de las comisiones de Comercio, Seguridad, Equidad y Género, Población Vulnerable y Derechos Humanos de la Cámara de Diputados y de Senadores.

→ Gobiernos Estatales: Distrito Federal, Jalisco, Baja California y Coahuila.

---

[37]Procuraduría General de la República, *El gobierno mexicano combate a fondo la explotación sexual infantil,* [en línea], México, Boletín no. 132, 10 de febrero de 2004, Dirección URL: http://www.pgr.gob.mx/cmsocial/bol04/feb/b13204.htm [consulta: 28 de mayo de 2010]

[38]PGR, *Informe Trimestral (Enero-Marzo 2004)*, [en línea, PDF], México, Procuraduría General de la República, Dirección URL: http://www.pgr.gob.mx/temas%20relevantes/Documentos/Informes%20Institucionales/1trimestre2004.pdf [Consulta: 28 de mayo de 2010]

→ Universidades y Centros de Educación Superior.

→ Empresas privadas vinculadas con seguridad en sistemas de cómputo, asociaciones nacionales e internacionales.

→ Organizaciones civiles comprometidas con la seguridad en Internet y de *e-comerce*.

→ Proveedores de servicios de Internet en México.

De hecho, de acuerdo con la dirección de Inteligencia de la SSP, uno de los objetivos de esta policía es la conformación de un banco de datos sobre pedofilia y agresiones sexuales. Lo cual será de utilidad para identificar patrones, rangos, preferencias y modus operandi de las bandas dedicadas a este ilícito. Este sería el primer banco de datos de bandas mexicanas dedicadas a la prostitución infantil realizado a través de Internet.

Cabe señalar que si bien entre sus funciones está la de combatir la pornografía infantil vía Internet, la Policía Cibernética también busca prevenir otros delitos, principalmente aquellos que atentan contra las instituciones y la población vulnerable. Otros ilícitos que persigue la policía cibernética mexicana son los fraudes, robos de información y suplantación de identidad:

> Con el objeto de endurecer e intensificar las acciones tendientes a disuadir los delitos cibernéticos como el fraude, el robo de señal a celular y el desvío electrónico de fondos bancarios a través de tarjetas de crédito o débito clonadas o con números robados, esta semana se urgió por establecer y consolidar todos aquellos mecanismos de colaboración para reforzar el monitoreo de incidencias delictivas[39].

[39] PGR, *Informe Trimestral*, *Ibid.*

A pesar de que hay un respaldo jurídico en la legislación mexicana, como ya se ha mencionado anteriormente, no hay una ley, al menos no de una manera específica, para la normatividad de los delitos informáticos como tal, la mayoría de los delitos que se comenten en Internet están considerados por diferentes leyes y considerados como una modalidad de otros delitos. Pero esto no ha sido suficiente:

> Tras celebrarse la Décima Sesión de trabajo del Grupo Interinstitucional de Combate a Delitos Cibernéticos DC México, cuyos esfuerzos coordina la Policía Federal Preventiva se puso de manifiesto la imperiosa necesidad de impulsar una franca coordinación y un acercamiento con el Senado de la República y la Cámara de Diputados a efectos de contar con los instrumentos legales que permitan hacer frente a la delincuencia organizada que, a través del anonimato, hacen de la red uno de sus mejores aliados.[40]

Continuando con la revisión de los resultados arrojados por la policía cibernética, también los ha tenido en materia de fraudes electrónicos, en el 2003, se habían presentado por lo menos 16 denuncias, cuyo *modus operandi* apenas variaba.

El tipo de fraudes que se denunciaron se relacionaban con la compra-venta de productos en algunos portales como mercadolibre.com y deremate.com, además de un fraude por 380 mil pesos[41].

Está claro que la intervención de la policía cibernética no sólo radica en la identificación de sitios fraudulentos o de pornografía, o bien, en la prevención de los mismos también se ha valido de los recursos electrónicos para perseguir otros como el flujo del dinero que procede del crimen organizado, lo cual no ha resultado una tarea sencilla por las mismas características de la red:

> Como consecuencia de la globalización de la economía, el desarrollo de la tecnología informática y la movilidad de los flujos de capital a través de la banca cibernética, desde y hacia casi cualquier punto del planeta, el rastreo, reconstrucción y aseguramiento de los recursos de procedencia ilícita se hace más difícil; para investigar y perseguir esos delitos

[40] PGR, *Informe Trimestral, Ibid.*
[41] *Ibid.*

> se diseño y aplicó una estrategia integral de planeación y dirección de las investigaciones a través de la formulación de hipótesis de actuación y el empleo de modernos avances científicos y tecnológicos para detectar, seguir, reconstruir y vincular los recursos con los delitos que los generaron[42].

Entre otros resultados arrojados, durante 2003, está la liberación de 31 órdenes de aprehensión en contra de operadores de lavado de dinero. Estas rutas llevaron al aseguramiento de bienes muebles, inmuebles, de 43,651,451.00 pesos y 746,276.00 dólares. Como bien hemos señalado Internet tiene alcances geográficos que han llevado a la colaboración internacional:

> En atención a una solicitud del gobierno español y en cumplimiento de las resoluciones 1333 y 1373 del Consejo de Seguridad de Naciones Unidas se investigaron personas vinculadas con la organización terrorista vasca ETA, asegurando cuentas bancarias por 899, 985.56 pesos[43].

Pero también la Policía Cibernética participó activamente en foros y grupos de trabajo interinstitucionales para atender problemas específicos como:

- La Atención de Instalaciones Estratégicas (GCIE); el Análisis Estratégico de Coordinación Interinstitucional en Materia de Seguridad Pública y Factores de Riesgo a la Gobernabilidad y Estabilidad Democrática (GAT); la Prevención y Control del Tráfico de Armas de Fuego, Municiones y Explosivos (GITA); la Atención de Grupos Armados, Terrorismo y Narcotráfico; el Combate a los Delitos Cibernéticos, y la Atención de las Movilizaciones del Consejo Agrario Permanente.[44]

- Reunión Intersecretarial del Grupo de Puertos y Servicios México-Guatemala (GPSM-G).

[42] PGR, *Informe Trimestral*, *Ibid.*
[43] *Ibid.*
[44] *Ibid.*

Finalmente, es necesario mencionar que la persecución de delitos cibernéticos aún está en el camino de consolidarse. Actualmente, están surgiendo algunas áreas como la informática forense, una disciplina relativamente joven que consiste en la investigación de los sistemas de información con el fin de detectar y obtener evidencias de la vulneración de los sistemas.[45]

Esta disciplina sería un gran paso para la investigación, persecución y castigo de los delitos informáticos. La finalidad de ésta es obtener evidencia que pueda ser tomada en cuenta para el castigo de un delito. Contar con una policía cibernética ya es un avance, pero perfeccionar las técnicas de investigación y recopilación de pruebas, sería el siguiente paso, es decir, dar cabida a disciplinas como la informática forense, que auxilien su trabajo.

¿En qué consiste el análisis forense? Al respecto nos explica el M. en Computación, Roberto Sánchez Soledad, quien en 2009, obtuvo el Certificado en análisis forense, GIAC Computer Forensic Analyst SANS.

> Básicamente trata de encontrar, o responder a las preguntas de: qué pasó, cómo pasó, si es posible saber quién lo hizo. Es el qué, cómo, cuándo, dónde. Cuándo un equipo es comprometido, es decir, que algo le pasa, que su seguridad fue violada, que cierta información fue modificada, borrada, copiada, entonces el cómputo forense trata de responder a todas esas preguntas.
>
> ¿La evidencia digital es válida en un juicio?
>
> Evidencia digital. Sí, siempre y cuando sea requerida por el ministerio público. Lo que sucede es que el juez solicita un perito informático para que proceda y responda a las preguntas. Uno como perito entrega la respuesta a las preguntas: qué es lo que sucedió, cómo sucedió, todas esas preguntas. Entonces con la orden puedes llegar y hacer el análisis para poder

[45] Elena Pérez Gómez, *¿Qué es la informática forense o Forensic?*, [en línea], España, MICROSOFT, Centro para Empresas y Profesionales, Dirección URL: http://www.microsoft.com/business/smb/es-es/legal/forensic.mspx [Consulta: 30 de julio de 2010].

responderlas y así es como son válidas. Si el juez, a partir de un peritaje, no logra determinar exactamente la causa del problema, puede solicitar un segundo peritaje.

En México, propiamente no existe un área o una carrera o especialidad en análisis forense, lo que existen son cursos. En el extranjero hay muchos. Aquí contamos con el Congreso de Seguridad, que también damos nosotros, aquí se da una parte de especialización en el análisis forense.

Se puede decir que sí hay personas capacitadas, pero es muy difícil encontrarlas. La verdad es un área o campo muy cerrado, en el cual sí es muy difícil crecer a nivel personal, por ejemplo, si tú tienes 50 peritos ahorita en el análisis forense, duplicarlos es un poco difícil porque lo primero que necesitas son ingenieros que conozcan la parte de seguridad y después especializarlos en el análisis forense, lo cual sí requiere bastantes años de capacitación[46].

[46] Entrevista, 11 de octubre de 2010.

CAPÍTULO II

LOS PORTALES DEL SISTEMA BANCARIO. LA BANCA ELECTRÓNICA. BANCA EN LÍNEA.

> Estamos en las puertas de una sociedad sin dinero efectivo y sin cheques; de una sociedad en la cual los fondos y toda aquella información financiera relacionada con la misma es trasferida electrónicamente con la ayuda de las computadoras y de los sistemas de telecomunicación. Podemos señalar a la EFT como uno de los cambios más importantes con los que se beneficia el conjunto de la sociedad[47].

Hasta el momento hemos hablado de la seguridad en Internet desde un punto de vista general. Pero ahora nos enfocaremos al ámbito específico de las instituciones bancarias y los servicios que ofrecen a través de Internet. Hablar de bancos e Internet nos remite necesariamente a temas como: la Seguridad de la Información, transacciones bancarias, comercio electrónico, dinero electrónico, ataques cibernéticos (como el *pharming* y el *phishing*) que es, justamente, lo que trataremos en este apartado.

La importancia de la banca electrónica, o la banca en línea, radica en la penetración que está teniendo en diversos ámbitos de la vida social. Desde las empresas hasta las personas realizan operaciones en línea con mayor frecuencia por las ventajas que ofrece el medio. Como explica Francisco Ceballos Blanco, vicepresidente de MercadoLibre.com México y secretario del consejo directivo de la Asociación Mexicana de Internet: "[Internet] estaba orientado a búsquedas de información y el uso del correo electrónico, pero ha evolucionado hacia las transacciones, compras y banca en línea, realizar trámites gubernamentales, la educación, investigaciones, entre otros"[48].

---

[47] Alberto R. Lardent, *Sistemas de información para la gestión empresarial: Planeamiento, Tecnología y Calidad*, Buenos Aires, Pearson Education, 2001, pp. 291.
[48] Aida Ulloa, "Día de Internet", [en línea], México, El Universal.com, 14 de mayo de 2007, Dirección URL: http://www.eluniversal.com.mx/finanzas/57755.html [Consulta: 10 de junio de 2010].

Pero ¿qué es la banca electrónica o banca en línea?

Escucharemos con frecuencia que para referirse a los servicios bancarios por Internet se utilizan indistintamente los términos: banca electrónica (*e-banking*), banca por Internet (u online) y banca virtual. Hasta el momento no hay una convención que establezca cual de todos es el correcto, pero en la mayoría de las referencias consultadas, el concepto más utilizado es el de banca electrónica y el que le sigue, banca en línea (u online). Por definición la más apropiada sería banca en línea, pues comprende aquellas herramientas que ofrece un banco para que sus clientes realicen operaciones por medio de una computadora con conexión a Internet.

Banca electrónica, es un concepto más general. Aquí se incluyen otros medios, aparte de Internet, como los cajeros automáticos, teléfonos fijos y móviles, u otras redes de comunicación. En el caso de la banca virtual sólo mencionaremos que es como se conoce a los bancos sin una presencia física, o sucursales, su presencia es absolutamente virtual. Aunque se asocia generalmente a la banca electrónica, no trataremos este tema, pues nos interesa la banca electrónica, o en línea, como un servicio que ofrecen las instituciones bancarias existentes en nuestro país. Además nuestro país aún no se empieza a transitar hacia esos terrenos.

Cuando hablamos de banca en línea, o banca electrónica, nos referimos al suministro de productos y servicios bancarios para consumidores, por medio de canales electrónicos, incluyendo el Internet. Estos productos y servicios pueden ser: la recepción de depósitos, préstamos, manejo de cuentas, asesoría financiera, pago electrónico de facturas, y el suministro de otros productos y servicios de pago como puede ser dinero electrónico[49].

[49] *s/a, Gestión de Riesgos para la banca electrónica y actividades con dinero electrónico* [PDF, en línea], Brasilea, Comité de Brasilea para la Supervisión Bancaria, marzo de 1998, Dirección URL: http://www.asbaweb.org/documentos/publicaciones/98-PUB-ESP-gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf [25 de mayo de 2010]

Hoy en día es mucho más sencillo realizar transacciones bancarias con unos cuantos clicks, que perder tiempo en largas filas de banco. Las instituciones bancarias han realizado algunos esfuerzos a fin de automatizar una importante cantidad de procesos, incluyendo entre sus servicios algunos que facilitan la realización de las operaciones bancarias que otorgan al usuario una mayor independencia para realizar transacciones.

De acuerdo con un estudio de la Asociación Mexicana de Internet[50] (AMIPCI) el 64 por ciento de los internautas utilizan algún tipo de servicio bancario: crédito hipotecario, crédito automotriz, cuentas de ahorro o nómina, tarjeta de débito o crédito, entre otros. En dicho estudio también se señala que el 67 por ciento de los encuestados utiliza o visita uno o más portales bancarios.

Pero ¿qué hacen los usuarios en un portal de Internet?, de acuerdo con el mismo estudio realizado por la AMIPCI encontramos que entre las actividades que más realizan los usuarios en los portales, están las siguientes[51]:

Actividad	%
Consulta de Saldo	87%
Transferencias a mis cuentas	68%
Transferencias a terceros	64%
Pago de servicios	63%
Pago de tarjetas de crédito	58%

[50] *Estudio AMIPCI de Banca por Internet en México 2007. Resumen Ejecutivo*, [en línea], México, Asociación Mexicana de Internet, 2007, Dirección URL: http://amipci.org.mx/estudios/temp/EstudioAMIPCIdeBancaporInternetenMexico2007RESUMENEJECUTIVO-095394800120352190 3OB.pdf [Consulta: 1 Junio de 2010]
[51] *Ibid.*

Pero si la banca electrónica resulta ser tan benéfica, o al menos una opción viable y cómoda al momento de realizar transacciones electrónicas, entonces ¿por qué no todos los usuarios acceden a él? Una de las respuestas es: la seguridad. En una de las preguntas del estudio de la AMIPCI, se les cuestionó lo siguiente: "¿qué necesitarías para realizar operaciones dentro de la banca por Internet?", casi la mitad de los encuestados respondió: Seguridad[52].

Un dato interesante es que el 94 por ciento de las personas entrevistadas conoce las medidas de seguridad que se deben seguir al momento de realizar en línea; mientras que el 83 por cierto considera que la seguridad es responsabilidad de las instituciones bancarias; y el 17 por ciento entiende que al momento de realizar operaciones de banca electrónica el usuario tiene un papel fundamental en la seguridad.

Lo cierto es que el desarrollo de la banca electrónica y el dinero electrónico tiende a mejorar la eficiencia del sistema bancario y de pagos; además de reducir el costo de las transacciones con los consumidores a nivel nacional e internacional. Sin olvidar que facilita el acceso al sistema financiero de los consumidores. No obstante, la seguridad sigue siendo el tema que limita de una forma u otra el pleno uso de estos servicios.

El interés de diversos organismos financieros como la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), la Comisión Nacional Bancaria y de Valores, y el Banco de México, es incentivar el uso de la banca electrónica. Una de las razones es la reducción de los costos y del tiempo que implica, como lo expresó Agustín Carstens, gobernador del Banco de México:

[52] *Estudio AMIPCI de Banca por Internet en México 2007, Ibid.*

> Los costos directos de transacción, de transportación, de tiempo, entre otros, se abaten considerablemente con el uso cada vez más generalizado de los medios electrónicos para liquidar pagos, en especial para las personas de menores recursos. Por ello, el Banxico intensificará la promoción de estos medios de pago a través de diversas estrategias y con todos los instrumentos de que dispone, además de que trabajará en coordinación con las diversas autoridades financieras del país"[53].
>
> Carstens añadió que para junio del año próximo año, requerirá a los bancos reducir el tiempo en que las transacciones se hacen efectivas en las cuentas de los beneficiarios a no más de un minuto… El Gobierno, dijo Carstens, también está tratando de migrar sus pagos, como nóminas del sector público federal a través de SPEI… México está tratando de reducir el uso de efectivo en su economía, en la que buena parte de las transacciones ocurren en el sector informal, en busca de hacer más eficiente el sistema de pagos y reducir la incidencia de delitos como el lavado de dinero de actividades ilícitas como el narcotráfico.[54]

Otra razón del interés por incrementar el uso de los sistemas de banca electrónica es que son considerados medios más seguros y confiables que el manejo de efectivo. Un poco contrario a la creencia de algunos usuarios, quienes aún no confían del todo en estos sistemas.

Como lo expresó Carlos López-Moctezuma, director general de Proyectos Especiales y Vocero de la Comisión Nacional Bancaria y de Valores: "Gran parte de la estrategia que ha tenido la CNBV en los últimos años es precisamente incentivar la bancarización y medios electrónicos, y paralelamente desincentivar el uso de efectivo […] Lo importante de las transacciones electrónicas es que son medios más seguros que el efectivo".[55]

---

[53] Notimex, "Ampliará bancos servicio electrónico", [en línea], México, El Universal.com.mx, 24 de mayo de 2010, Dirección URL: http://www.eluniversal.com.mx/notas/682655.html [consulta: 24 de mayo de 2010].
[54] s/a, "México extenderá horario de sistema de pagos electrónicos", [en línea], México, Agencia Reuters, 24 de mayo de 2010, Dirección URL: http://www.reuters.com/article/idARN2426140420100524 [Consulta: 24 de mayo de 2010]
[55] Notimex, "CNBV apoya disminuir uso de efectivo", [en línea], México, El Universal.com.mx, 24 de mayo de 2010, Dirección URL: http://www.eluniversal.com.mx/notas/682688.html [consulta: 24 de mayo de 2010].

Paulo Carreño, director de comunicación de Banamex comentó lo siguiente: “Vemos con muy buenos ojos y, por supuesto, seguiremos con toda atención cualquier iniciativa que permita trasladar las operaciones financieras a medios más eficientes, modernos y seguros”[56]. Esta seguridad está relacionada con la disminución del uso de efectivo en operaciones que pueden prestarse a actividades ilícitas:

> El presidente de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), Luis Pazos, dijo que el objetivo teórico de realizar transacciones como la adquisición de bienes inmuebles y automóviles por medios electrónicos y no en efectivo es bueno, para evitar el lavado en el caso de las grandes operaciones.[57]

SEGURIDAD

> *Las tres inquietudes más importantes para una red de comercio electrónico son los niveles de seguridad, la sencillez, y la eficiencia en los costos[58].*

Internet es una red pública y existe una constante amenaza contra la seguridad de la información de los usuarios de la banca. Internet, en general, tiene problemas de autenticidad, integridad, confidencialidad y repudio afectando a los requerimientos de las transacciones electrónicas u operaciones de banca virtual de la siguiente forma[59]: Robo de información, suplantación de identidad, sniffers, modificación de información, repudio, denegación del servicio.

---

[56] *Ibid.*
[57] s/a, “Recomienda Condusef realizar transacciones electrónicas”, [en línea], México, El financiero, 25 de mayo de 2010, Dirección URL: http://www.elfinanciero.com.mx/ElFinanciero/Portal/cfpages/contentmgr.cfm?docId=264284&docTipo=1&orderby=docid&sortby=ASC [Consulta: 25 de mayo de 2010]
[58] Toby J. Velte, *Fundamentos de comercio electrónico*, México, Ed McGraw-Hill, serie Biblioteca Profesional, 2001, pp. 355.
[59] Jordi Buch i Tarrats, *ibid.*

> La integridad de los datos es un concepto utilizado para describir su estado en relación con su pérdida o corrupción. Una integridad de datos pobre implica que dichos datos pueden ser incorrectos o incompletos. La seguridad hace mención a las propiedades de la semántica de los datos en relación con una autoridad que debe ser considerada como propietaria (emisor y/o receptor).[60]

Para hablar de seguridad en los portales bancarios, tenemos que hablar de los EFT: "Se entiende por EFT cualquier método de transferir dinero (débito o crédito) de una cuenta a otra por medios electrónicos (telecomunicaciones), sin necesidad de generar y procesar un documento (papel) para autorizar la transacción"[61]

Tal vez haya escuchado alguna vez algo como: "no proporcione información confidencial a páginas de las que desconfíe", o bien, "los bancos no solicitan información a través de correos electrónicos". Esto se debe a dos actividades que se desarrollaban en la WEB, el *pharming* y el *phishing*. Ambas vinculadas al fraude, cuyo objetivo es la obtención de beneficios económicos e información privilegiada[62]. Ya en el capítulo primero nos adelantábamos al concepto de delito cibernético, bien, aquí hablaremos más específicamente de dos.

El *phishing* corresponde a los delitos de robo de información, se valen del engaño para obtener datos de la víctima que posteriormente utilizan. Al principio era sencillo que cayeras en el engaño, pues se desconocía cómo operaban.

> El *phishing* consiste en el envío de mensajes (anzuelos) a unas o varias personas, recurriendo a la suplantación de la identidad de una empresa o entidad pública con el objetivo de persuadir a la futura víctima para revelar sus datos personales o financieros que involucran nombres de usuario y contraseñas. Una vez obtenida esta información es utilizada con fines maliciosos para realizar acciones con transferencias de fondos a cuentas

[60] Juan Francisco Puentes Calvo, *Principios de seguridad en el comercio electrónico,* México, Ed Alfaomega Ra-Ma, colección Navegar en Internet, 2009, pp. 87.
[61] Alberto R. Lardent, *op. cit.* 291
[62] Juan Patiño Corona, "Pharming, la evolución de un Ataque", [en línea], México, Punto Seguridad-Defensa Digital, UNAM, Número 2, Agosto 2009, Dirección URL http://revista.seguridad.unam.mx/rs_unam_02/001_03/art_03.html [Consulta: 03 de mayo de 2010]

bancarias y compras con tarjetas de crédito entre otras acciones delictivas que afectan económicamente a la víctima[63].

Hay diferentes formas de *phishing*[64]:

TIPOS DE PHISING	
Deceptive *Phishing*	Consiste en el envío de correo electrónico engañoso en el que se suplanta a una empresa o institución de confianza, de esta forma la víctima al pulsar el enlace contenido en el mensaje, es redireccionado de manera inconsciente aun sitio Web fraudulento.
Malware Based Pishing	La variante en este tipo de *phishing*, implica la ejecución de un software de un código malicioso en el equipo de la víctima ya sea como resultado de abrir un archivo adjunto en un mensaje, visitar una página Web, descarga de un programa. Ejemplos de ello son las herramientas como los *keyloggers* y los*screenloggers*, los primeros registran las pulsaciones del teclado y estos datos son grabados por el programa y reenviados al atacante, la segunda herramienta realiza lo mismo pero mediante la captura de imágenes de la pantalla.
DNS Based *Phishing* (*Pharming*)	Este delito interfiere en el proceso de búsqueda de los nombres de dominio, es decir modifica de forma no autorizada la resolución del nombre de dominio enviando al usuario a una dirección IP distinta.
Content-Injection *Phishing*	Este tipo de ataque consiste en introducir contenido fraudulento dentro de un sitio Web legítimo.
Made-in-the-Midle *Phishing*	Usando esta técnica el atacante se posiciona entre el ordenador del usuario y el servidor, de esta forma puede leer, filtrar y modificar la información a la que tiene acceso.
Search Engine *Phishing*	Los atacantes crean páginas Web con ofertas atrayentes para los usuarios, estas páginas se encuentran indexadas legítimamente con los motores de búsqueda, de tal forma que el usuario las encuentra y debido a lo atrayente que resultan las ofertas mostradas proporciona su información.

Fuente: Punto Seguridad-Defensa Digital, UNAM

[63] Miriam J. Padilla Espinosa, "Pescando Información *Phishing*", [en línea], México, Punto Seguridad-Defensa Digital, UNAM, Número 2, Agosto 2009, Dirección URL: http://revista.seguridad.unam.mx/rs_unam_02/001_02/art_02.html [Consulta: 03 de mayo de 2010]
[64] *Ibid.*

Por otro lado, el *pharming* es un ataque similar al *phishing* pero recargado, o mejor dicho, con un mayor alcance. La intención del *pharming* es direccionar a los usuarios a sitios maliciosos que son clones de páginas oficiales. Por ser idéntica a la página original, sin que el usuario se percate de ello, ingresa información confidencial (usuario y *password*):

> El fraude es hoy en día uno de los crímenes que encabeza la lista de delitos informáticos en nuestro país y los objetivos del *pharming* en su mayoría se dirigen a obtener beneficios económicos e información privilegiada, muchas veces para la generación de estafas. Este tipo de ataque generalmente busca la obtención de: Información bancaria, credenciales de acceso (nombre de usuarios y contraseñas), información personal (números telefónicos, direcciones, e-mail, etc.). Es importante recalcar que en la mayoría de los casos el *pharming* se dirige a la creación de fraudes, pero tiene un campo de acción mayor, por ejemplo, puede emplearse para dirigir a los clientes de un DNS comprometido a páginas web donde se les descargará código malicioso forzando la generación de visitas en algún sitio cuando los clientes tecleen la dirección de algún portal conocido valiéndose de su popularidad.[65]

Lo peligroso de este tipo de ataque es que no se ataca de manera individual, sino que puede llegar a afectar a redes completas, dato que resulta importante para las empresas que manejan redes en su estructura. Y justamente es aquí la diferencia entre ambos ataques, el *phishing* afecta de manera individual, cada usuario es captado por medio de correo electrónico; mientras que *pharming*, puede afectar toda una red, tan grande como la cantidad de clientes del Servidor DNS (Servidor de Nombres de Domino, por sus siglas en inglés).

> El *pharming* va más allá ya que puede afectar a máquinas de manera individual o a redes enteras que hagan uso del mismo servidor DNS o dispositivo comprometido, lo que permite que el atacante tenga bajo su control a un grupo de usuarios vulnerables tan grande como la cantidad de clientes del Servidor DNS contaminado lo que resulta más peligroso, pues mientras el *phishing* requiere que cada usuario acceda al link del estafador para convertirse en víctima, el *pharming* sólo necesita que alguien haga una consulta legítima al servidor

[65] Juan Patiño Corona, *ibid.*

DNS modificado, haciendo que muchas precauciones tomadas para protegerse del *phishing* no sean suficientes ni útiles para evitar el *pharming*.[66]

CANDADOS

A fin de conservar la seguridad se han desarrollado algunos candados se seguridad, sin entrar en detalles técnicos, explicaremos algunos de los más utilizados:

- **Certificado digital**. Consiste en una certificación electrónica que es generada por una autoridad con base en la vinculación entre datos de verificación de firma y un signatario, la correspondencia de ambos es la que valida la identidad. El certificado tiene una validez determinada y un uso concreto. Por ejemplo, las claves que proporcionan las instituciones bancarias, las cuales vienen almacenadas en un dispositivo que otorgan al usuario. Esas claves se utilizan una sola vez y con un fin determinado.

- **Firma electrónica avanzada**. Es un conjunto de datos que identifican a un usuario en particular. Esta identificación única permite la identificación del usuario. Debido a que la firma es creada por medios que el usuario mantiene bajo su exclusivo control, hay una garantía de seguridad importante, pues está vinculada únicamente al mismo y a los datos que se refiere, lo que permite la detección de cualquier modificación. Actualmente, algunas instituciones gubernamentales como el Servicio de Administración Tributaria validan el uso de firmas electrónicas para la impresión de facturas, con lo que el usuario puede generar documentos digitales con validez oficial. La meta es incrementar el uso de estos medios.

- **Criptografía**. Es “un conjunto de técnicas y estándares que permiten la identificación electrónica de una entidad, firmar electrónicamente y cifrar

[66] Juan Patiño Corona, *ibid.*

datos”[67]. Implica el uso de dos claves: una privada y una pública. El objetivo de esta modalidad es la codificación del mensaje entre el emisor y receptor, de tal manera que ningún intruso pueda interpretar el contenido real.

> Entre los objetivos de una comunicación segura, además de la ya supuesta confidencialidad de datos, se encuentran la autentificación, el control de accesos, su integridad y el no repudio sobre los mismos. Para poder llevarlos a cabo los criptógrafos desarrollan algoritmos cifradores, que los criptoanalistas intentan romper… Los criptoanalistas se plantean tres puntos posibles de partida para llevar a cabo su labor: tener una determinada cantidad de texto cifrado, pero sin poseer texto claro; poseer tanto parte del texto cifrado como su correspondiente normal; y por último el criptoanalista puede tener la capacidad de generar texto cifrado a partir del texto claro, por él seleccionado.[68]

- ***Secure Sockets Layer* (SSL)**: “Es un protocolo que permite la autentificación mutua de un usuario y un servidor con el propósito de establecer una conexión cifrada”[69].

- ***Secure Electronic Transaction* (SET)**: “Protocolo que asegura la confidencialidad y la integridad de los pagos basados en tarjeta hechos por Internet, con independencia de quien sea el comprador y el vendedor del producto. El protocolo garantiza la autenticidad de las partes”[70].

- **Infraestructura de Clave Pública (PKI)**. Son los estándares, servicios y certificados que facilitan el uso de la criptografía en un entorno de red.[71]

En la banca electrónica, los clientes realizan transacciones sobre la redes TCP/IP, que es la referente a Internet, WAP (comunicaciones móviles) o propietaria, aquí se

[67] Jordi Buch i Tarrats, *ibid.*
[68] Juan Francisco Puentes Calvo, *op. Cit. p.* 25.
[69] Jordi Buch i Tarrats, *ibid.*
[70] *ibid.*
[71] *ibid.*

incluyen a los cajeros automáticos. La banca por Internet distingue, para efectos de seguridad, entre la autentificación del usuario y la autorización de transacciones.

SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS (SPEI)

Un avance importante en materia de transferencias electrónicas es el Sistema de Pagos Electrónicos Interbancarios (SPEI). Este sistema fue desarrollado por el Banco de México, que es el banco central de la Nación, y la banca comercial (instituciones bancarias del país); el objetivo de este sistema es la transferencia electrónica de dinero de manera segura, rápida y cómoda.

> Esta opción de transferencia de fondos es bastante segura para el usuario, ya que tiene el respaldo de la seguridad de la banca electrónica, resaltó el autor del libro *Informática para no informáticos*. Lo importante, dijo, es que los cuentahabientes entiendan de manera clara los pasos para realizar el proceso e identifiquen y se familiaricen con el lenguaje bancario que se utiliza. Sin embargo, aclaró que los usuarios de la banca sólo utilizarán los medios electrónicos como Internet, si se sienten seguros y preparados para ello, de lo contrario seguirán acudiendo a las sucursales bancarias a realizar sus transacciones. Gutiérrez Garay comentó que para asegurar la adopción de estas tecnologías, el siguiente paso es estandarizar el conocimiento de la computadora y el Internet entre los mexicanos. Esto, agregó, permitirá tener una referencia de aprendizaje para los ciudadanos y las organizaciones que digitalicen sus procesos, como es el caso del sistema financiero[72].

No obstante, aún tenemos algunas carencias para que este tipo de sistemas funciones al cien por ciento en México, una de las carencias más notables es el acceso a Internet como lo plantea Sergio Gutiérrez Garay, autor del libro *Informática para no informáticos*:

> El Sistema de Pagos Electrónicos Interbancarios (SPEI) es una excelente muestra de los avances de la banca electrónica en México, sin embargo, el poco acceso a Internet en el país aún lo hace inaccesible para gran parte de la población. Y es que, en México sólo 23%

[72] s/a, “Avanza banca electrónica en México”, [en línea], México, ElUniversal.com.mx, 10 de abril de 2009, Dirección URL: http://www.eluniversal.com.mx/articulos/53468.html [consulta: 24 de mayo de 2010]

> de la población usa Internet y esta cifra se reduce si consideramos sólo a los internautas que tienen cuentas bancarias, pues únicamente 50 por ciento de ellos usa la banca en línea.
>
> Se esperaría que con una nueva Ley para el Desarrollo de la Sociedad de la Información, aprobada por la Cámara de Diputados, se facilite el acceso a la computadora y el Internet, y así más usuarios se beneficien de la banca electrónica. El SPEI es utilizado por 60 instituciones financieras del país, de ellas 44 son bancos y el resto entidades como casas de bolsa, de cambio, Afores y aseguradoras. Además de simplificar el proceso de transferencias electrónicas, por medio del SPEI, el Banxico busca alentar a la población para que disminuya el uso de medios de pago como el cheque o el efectivo, que representan un mayor riesgo y costos indirectos.[73]

¿Cómo funciona el SPEI?

El funcionamiento general es el siguiente: El ordenante (que es la persona que desea transferir el dinero desde una cuenta bancaria) instruye a su banco que transfiera "x" cantidad a través del servicio de banca en línea. En la instrucción se indica el monto de la transferencia y los datos del beneficiario (es la persona física o moral que recibirá el monto), los datos que se solicitan son el nombre, la cuenta CLABE, la cual consiste en 18 dígitos (o en su caso el número de la tarjeta de débito) y el nombre de la institución bancaria a la que pertenece la cuenta receptora.

También tiene la opción de incluir alguna referencia (7 dígitos) o concepto (40 letras o dígitos) para una mejor identificación de la transferencia. Hasta el momento hay varias certificaciones que tienen que validar la operación, con lo que nos podemos dar cuenta del nivel de seguridad que se lleva a cabo para proteger tanto al ordenante como al beneficiario. Pero aquí no termina. Al recibir la instrucción, el Banco Emisor (el del ordenante) verifica la identidad de su cliente y que el saldo en su cuenta sea suficiente para cubrir la transferencia. Cumpliendo con estos requisitos se valida la operación.

[73] s/a, "Avanza banca electrónica en México", *Ibid.*

Una vez validada la identidad y el saldo, el Banco Emisor confirma al Ordenante, vía Internet, la hora precisa en que aceptó la transferencia, así como una clave de identificación única, llamada "número de rastreo", la cual sirve para futuras aclaraciones. Minutos después (sí, minutos), el Banco Emisor transmite a través del SPEI toda la información de la transferencia al Banco de México; el cual, al recibirla transfiere el dinero de la cuenta emisora hacia la cuenta que le lleva el Banco Receptor y retransmite, también a través del SPEI, toda la información necesaria al Banco Receptor. De esta manera, el Banco Receptor cuenta con la información necesaria y los recursos para depositarlos a favor del Beneficiario. Como veremos son varias etapas en el proceso para validad una transferencia.

Actualmente, SPEI es utilizado por 60 instituciones financieras del país, bancos y entidades como: casas de bolsa, de cambio, Afores y aseguradoras. La razón por la que cada vez más instituciones bancarias lO utilizan y Banxico la promueve, es porque pretenden disminuir medios de pago como el cheque o el efectivo, que representan un mayor riesgo y costos indirectos. Entre los bancos que utilizan este sistema (al momento de la realización de esta investigación) están[74]:

- AFIRME
- AZTECA
- BAJIO
- BANAMEX
- BANJÉRCITO
- BANK OF AMERICA
- BANK OF TOKYO
- BANORTE
- BANREGIO
- BANSI

[74] *Vid* Dirección URL: http://www.banxico.org.mx/sistemasdepago/servicios/spei/Bancos.html [Consulta: 1 de junio de 2010]

- BBVA BANCOMER
- HSBC
- INBURSA
- INTERACCIONES
- INVEX
- IXE
- JP MORGAN
- MIFEL
- MONEX
- MULTIVA
- SANTANDER
- SCOTIABANK
- THE ROYAL BANK OF SCOTLAND (RBS)
- VE POR MÁS

EL COMERCIO ELECTRÓNICO.

¿Cómo adquirimos algún producto o servicio por Internet? Uno de los medios que está tomando fuerza para realizar una compra en línea es la transferencia electrónica, aunque no es la única. Hay una perspectiva que nos permite considerar al comercio electrónico como una alternativa viable y, por ende, la transferencia electrónica como el medio de pago.

> Los instrumentos de pago facilitan el intercambio de bienes y servicios, y responden a necesidades específicas. Los medios utilizados varían de un país a otro: efectivo (monedas y billetes), cheques, transferencias de crédito, débitos directos, trasferencias interbancarias, tarjetas de pago, etc., […] Observando las diferentes preferencias de medios de pago de

> cada país se ve claramente cómo las técnicas de comercio electrónico deben contemplar el comportamiento social y las tendencias de los diferentes estados[75].

El reto para las instituciones bancarias se incrementa, pues ahora tienen que considerar, no sólo la seguridad de los usuarios al momento de ingresar a sus portales con el fin de realizar transferencias, pagos, consultas, entre otros; además se amplía el espectro de posibilidades al hablar del comercio electrónico, pues al adquirir productos a través de Internet y realizar pagos por el mismo medio y utilizar información (como números de cuenta, por ejemplo) para realizar esas operaciones, es menester considerar la seguridad de los medios utilizados por los usuarios como tarjetas de crédito. Por ello es necesario hablar del comercio electrónico, el cual podemos definir como: "la actividad comercial consistente en la entrega de bienes, o servicios, a compradores que usan sistemas de pagos electrónicos (EPS)"[76].

En general, todas las transacciones o relaciones de carácter electrónico tienen en común el uso de una red de comunicaciones, ya sea pública (como Internet), o privada, como: la red GSM, GPRS, o UMTS de la operadora móvil del cliente. Otro punto en común es que una de las partes, o todas ellas, tienen un interés especial en ocultar alguno o todos los datos de la transacción.[77]

Como usuarios conocemos los problemas propios de los sistemas de pagos tradicionales como el efectivo, entre los que destacan: la falsificación, las firmas olvidadas, o bien, que los cheques sean rechazados, etc. De la misma manera, los EPS, tienen sus propios problemas[78]:

1. Los documentos digitales pueden ser copiados con exactitud y frecuencia.

[75] Juan Francisco Puentes Calvo, *op. cit.114*.
[76] *Ibid,* p. 117.
[77] *Ibid, p.* 118.
[78] *Ibid,* p. 119.

2. Las firmas digitales pueden ser generadas por cualquiera que conozca la clave privada.

3. La identidad usuario puede ser asociada con cada transacción que realice.

Por lo que los requerimientos de seguridad de los EPS se fundamentan en cuatro principios fundamentales: autentificación, integridad, autorización y confidencialidad[79].

1) La autentificación. Ambas partes deben comprobar su identidad.

2) La integridad de la información. Es necesario salvaguardar los datos implicados en las transacciones.

3) La autorización. Con esto se pretende garantizar que las transacciones deberán ser manifiestamente consentidas por parte del usuario.

4) La confidencialidad. Se refiere al deseo de alguna, o de todas las partes, de alcanzar la imposibilidad de rastrear la transacción o que su identidad no sea asociada con la misma. Como ya hemos dicho, la autentificación y la confidencialidad no son excluyentes.

Aunque estos principios se asocian al comercio electrónico, también son un fundamento esencial en el caso de las transacciones bancarias, pues estamos hablando de información confidencial. El banco está obligado a la conservación de la integridad y confidencialidad que los usuarios proporcionan.

Como mencionábamos al principio no se puede hablar de banca en línea sin tomar en cuenta un tema importante: el comercio electrónico. La razón principal es que la

[79] Juan Francisco Puentes Calvo, op. Cit. P. 119.

mayor parte de los pagos que se realizan en el comercio electrónico son a través de transferencias electrónicas. El crecimiento que ha tenido este sector también ha influido directamente en el uso de la banca en línea.

Al ver datos como los que ofrece la Asociación Mexicana de Internet, en el que las ventas totales del comercio electrónico en 2008 alcanzaron mil 768 millones de dólares, basados únicamente en la oferta de los comercios mexicanos, nos damos cuenta de la relevancia que está adquiriendo este medio de compra-venta.

> Las ventas totales del comercio electrónico al consumidor alcanzaron 1,768 millones de dólares en el 2008, basados únicamente en la oferta de los comercios mexicanos. Esto evidencia el continuo crecimiento del sector, ya que este año registró un aumento del 85% en sus modalidades B2C (negocio a consumidor) y C2C (entre consumidores).[80]

El comercio electrónico en México presenta un fuerte crecimiento y todavía existe mucho hacia donde crecer, sus ventajas son cada vez más reconocidas, e incluso durante este periodo de retos económicos más gente se unió al *e-commerce* para encontrar mejores precios y oportunidades, como lo visualizó Francisco Ceballos, Vicepresidente del Comité de Comercio Electrónico y Director General de Mercado Libre México.[81] Mauricio Braverman, Director Ejecutivo de Productos para Visa México, también previó dicho crecimiento:

> De acuerdo al estudio, un 74% de las compras en Internet se realizan con tarjeta de crédito. Es claro que el dinero electrónico contribuye al desarrollo acelerado del comercio electrónico, promueve el progreso y facilita modelos de negocio que en el pasado no eran viables. La oportunidad ahora es habilitar que las tarjetas de débito también se usen de manera masiva y con seguridad en este canal. Esto permitirá que millones de mexicanos

[80] s/a, "El comercio electrónico en México facturó 1,768 millones de dólares en 2008: AMIPCI" [en línea], México, AMIPCI, 14 de octubre de 2009, Dirección URL: http://www.amipci.org.mx/prensa/temp/BoletindePrensaComercioElectronico-08451660012555460 53OB.pdf [consulta: 1 de junio de 2010]
[81] *Ibid.*

> utilicen en Internet un medio de pago que ya poseen y con eso, se siga fomentado el crecimiento de esta industria[82].

En el estudio realizado por la AMIPCI[83] se demuestra un aumento en el porcentaje de las ventas internacionales, las cuales representan el 14 por ciento; mientras que al interior de la República son el 50 por ciento, lo que puede ser un reflejo de la "confianza generalizada que tienen los usuarios en el país y en el extranjero al hacer compras en línea en comercios en México"[84].

Pero ¿cómo está la confianza de los consumidores en cuanto a la seguridad al momento de adquirir algún producto o servicio a través del comercio electrónico? Según la encuesta, el 66 por ciento de los usuarios prefieren adquirir los productos o servicios en sitios de Internet reconocidos o recomendados, aquí se puede confirmar que no hay mejor publicidad que la que se da de boca en boca. Pero continuando, el 81 por ciento de los compradores buscan que las políticas de devolución y garantías se expresen claramente, que la información y las condiciones de compra-venta queden libres de toda duda.

Y buscando también que los lugares donde se adquieren productos estén avalados por alguna institución, el 68 por ciento de los usuarios declararon tener confianza al ver el Sello de Confianza de la AMIPCI. Pero también, buscan tener un referente físico, un dato destacado es que el 90 por ciento de los usuarios del comercio electrónico compara precios en tiendas físicas y/o en Internet antes de realizar cualquier compra.

Otro dato que revela la confianza de los usuarios es que el 77 por ciento de los consumidores que han comprado, volverían a adquirir productos en Internet lo cual nos señala que hay un alto nivel de satisfacción. Por supuesto que toda esta

[82] s/a, "El comercio electrónico en México facturó 1,768 millones de dólares en 2008: AMIPCI", *Ibid.*
[83] *Ibid.*
[84] *Ibid.*

información está basada en uno de los canales de comercio electrónico más conocido que es Mercado Libre.

CREANDO CONFIANZA EN EL USUARIO

No existen sistemas 100% seguros, salvo los que están apagados. Es indispensable que las instituciones bancarias, proporcionen todos los elementos que garanticen la seguridad de la información de los usuarios en sus operaciones. Además, es responsabilidad del banco proporcionar la información al usuario de cómo utilizar los servicios e la banca en línea, para evitar errores que signifiquen pérdidas. Pero ¿qué elementos debe considerar el usuario para determinar si un sitio es seguro o no?

El maestro Roberto Sánchez Soledad nos habla de la difusión de una cultura en Seguridad, o bien buenas prácticas de seguridad:

> Hay muchas recomendaciones en la red, que son más buenas prácticas de seguridad. Nosotros llevamos lo que es un programa de concientización al usuario, la cual requiere que cumplamos con algunas políticas, por ejemplo, no usar software pirata, todo mundo acostumbra en México usar un Windows pirata, esa es una muy mala práctica de seguridad, luego no sabemos qué la pasó al sistema operativo.
>
> Los antivirus son buenos, son la primera barrera que un usuario tiene, el problema es que muchas veces no los tenemos actualizados, por lo mismo, que tenemos un antivirus pirata. Entonces, el primero de ellos es tener nuestro sistema operativo original, actualizado, esto es muy importante, si tu software es original ellos te proporcionan las actualizaciones gratuitas.
>
> Si tienes tu antivirus debes tenerlo activado, muchas veces los usuarios dicen “tengo mi antivirus pero me alenta la máquina, así que lo desactivan que es lo mismo a no tenerlo. La tercera es tenerlo actualizado, todos los días salen virus diferentes y los antivirus se actualizan diariamente.

Otra recomendación es manejar contraseñas. Tengo mi máquina, tengo mi usuario (el cual puede ser mi nombre o cualquier cosa que quieras poner) y una contraseña. La mayoría de los usuarios no acostumbramos usar password, porque pensamos: “Es mi máquina, sólo yo la uso”, pero al conectarnos al Internet, cualquier persona con conocimientos suficientes pueden meterse a mi máquina y si no tienen *password* es más fácil.

También se recomienda cumplir políticas en el *password*, por ejemplo cumplir con longitudes mínimas, 8 caracteres, números, letras, mayúsculas, minúsculas, una combinación de letras que podamos recordar. Serían mis recomendaciones más.

Otra buena práctica de seguridad, no realizar transferencias bancarias en cafés Internet eso es muy común, sobre todo en aeropuertos u otros lugares, porque tú llegas a un equipo y metes información confidencial en el equipo (tu nip, tu token, por ejemplo) y ahí te puede robar todo tu dinero.

La Cultura en Seguridad es difundir las buenas prácticas en seguridad para los usuarios. Si a nosotros nos educan a que nuestro equipo debe ser origina, debemos actualizar, que debemos manejar *passwords* fuertes, cuando llegamos a una nueva empresa, a nuestra casa, vamos a seguir esa cultura que nos inculcaron. Al seguir esas buenas prácticas somos menos propensos a sufrir algún *hackeo*, cualquier fraude, intrusión, reducimos el riesgo.

Capítulo III

LA RESPONSABILIDAD DE LOS USUARIOS EN LA SEGURIDAD. ¿Y YO POR QUÉ?

Probablemente en este punto de la historia nos preguntamos ¿qué tan seguro puede ser navegar en Internet?, ¿podemos confiar en proporcionar nuestra información confidencial a un portal?, conociendo que las instituciones bancarias utilizan ciertos sistemas que protegen esa información ¿se animaría a realizar transacciones por este medio, o bien, una compra por Internet?, ¿entraría a la dinámica de las compras por Internet?

El incremento del uso de Internet y del acceso a las nuevas tecnologías, nos hablan de que debemos aprender a convivir con ellas y, sobre todo, cómo utilizarlas. Conocer cómo funcionan disminuye, en gran medida, los riesgos al momento de enfrentarnos a ellas. Incluso se puede hablar de generar una cultura tecnológica, y evitar el "analfabetismo informático" que es como se conoce a las personas que no están instruidas en el tema. El objetivo, entonces, es aprender cómo funcionan para evitar ser víctimas de un delito informático. La información y el conocimiento es la mejor arma de la que disponemos para evitarlos.

Hasta el momento hemos identificado que aunque la seguridad en Internet es responsabilidad de los proveedores de servicios, ésta depende de tres actores principales:

→ **El Estado.** Es el que a través de distintas instituciones genera el marco legal que permite respaldar a los usuarios y de garantizarles que recibirán el apoyo en caso de que sean víctimas de un delito. Además es quien mantiene una relación con otros gobiernos para asegurar las medidas legales necesarias para garantizar esto.

→ **La institución bancaria.** Es la encargada de mantener la seguridad de los portales, evitar el acceso a las bases de datos de los usuarios. También deben de instruir a sus usuarios en los procedimientos elementales que le garantizan una navegación segura.

→ **El usuario.** Es, finalmente, el más interesado en que toda esta cadena funcione, pues será el más perjudicado en caso de que algo falle. Y es, finalmente, una de las piezas clave en todo esto.

De aquí la importancia de entender qué papel juega cada uno y qué medidas se deben seguir por parte de cada uno de los eslabones de la seguridad. Ya en el capítulo uno, hablamos ampliamente de la responsabilidad del Estado, a través de las leyes, las normas y la formación de grupos como la policía cibernética. En el amparo a nivel de jurisdicción de los ciudadanos.

También hablamos de las instituciones bancarias. Responsables de establecer sistemas seguros para los usuarios. Además de participar en la comprobación y validación de los usuarios al momento de efectuar una operación a través de Internet, por ejemplo, el comercio electrónico. Es momento de referirnos al usuario.

SISTEMAS OPERATIVOS DÉBILES

No obstante es menester conocer qué pilares se pueden flanquear para ingresar a nuestra información personal. Primero, como usuario le interesará conocer que los protocolos, es decir, las convenciones que se establecen sobre los formatos y reglas que se deben cumplir para la transmisión de información a través de Internet, fueron diseñados para que fuesen simples, sencillos y amables para el usuario.

Pero al intentar conseguir esta sencillez, se dejó de lado un aspecto importante: la seguridad. Es posible que los administradores de estos sistemas también tuvieran su parte de responsabilidad en esta historia:

> Los administradores de sistema por dejadez, desconocimiento y, generalmente, por falta de tiempo, no cuidan los posibles agujeros de seguridad existentes en los sistemas y en las comunicaciones. En algunas organizaciones, los administradores del sistema son los responsables de establecer la política de seguridad de la organización, y de educar a los usuarios de sus sistemas para que se conciencien en los problemas que implica la inseguridad. [85]

Lo que no implica dejar de considerar que en el usuario "también por dejadez o desconocimiento no ponen los medios adecuados para evitar que su información quede al acceso de usuarios no autorizados"[86]. Comenzaremos, entonces, por señalar que son tres los pilares fundamentales, al menos los que hemos identificado hasta el momento, de la seguridad:

- **Confidencialidad:** la información no debe ser visible para los ojos no autorizados.
- **Integridad:** La información no debe ser modificada por personas no autorizadas.
- **Disponibilidad:** La información debe estar siempre al acceso de sus propietarios.

Pero la base sobre la que descansa toda seguridad es la correcta configuración de los sistemas y las comunicaciones y, sobre todo, el seguimiento día a día, ya sea

[85] José Luis González S; Marisol Sánchez A; Alfonso Gazo C., *Autopistas de la Información e Internet: Tecnología, Servicios, Peajes y Normas de Navegación*, Universidad de Extremadura servicio de publicaciones, 1998, p. 402-403.
[86] *Ibid.*

como responsables de los sistemas o como usuarios finales de los mismos, que permita detectar, en todo momento, cualquier amenaza o incidente relacionado con la inseguridad de la información[87].

En conjunto, debemos desarrollar una cultura digital. Sabemos que estamos en una era donde el uso de la computadora es inevitable y es una habilidad que debe ser adquirida, pues ayuda a agilizar muchos procesos. Además el tener acceso a las computadoras y a Internet reduce costos e incrementa la productividad como ya hemos señalado.

El estudio realizado por la Asociación Mexicana de Internet, se estima que hoy en día hay 30.6 millones de internautas[88], cifra que se prevé incremente considerablemente y en ello podemos estar de acuerdo, al menos parcialmente, pues aún existen muchos elementos que pueden frenar esto, como los recursos, los costos que implica contar con una computadora y una conexión a Internet.

En cambio también se habla de una reducción de costos y mayor seguridad, al momento de considerar a Internet como un medio para la realización de transacciones bancarias, como lo consideran instituciones como el Banco de México o la Comisión Nacional Bancaria y de Valores.

Volvamos a plantear la siguiente pregunta: "¿Qué hacen los usuarios en la red?" Como hemos visto los usuarios realizan diversas actividades, como lo mencionábamos en el capítulo II, la diversificación de este medio, el Internet, ha permitido que los usuarios tengan acceso a aplicaciones de diversa naturaleza que van desde: las redes sociales, páginas personales, grupos o foros de discusión, consulta de información (como los diarios digitales), descargas de música, videos,

[87] José Luis González S, *op. cit., p.397*.
[88]Verónica Valencia, "Crece internautas 11% desde 2008", [en línea], Distrito Federal, Reforma.com, 17 de mayo de 2010, Dirección URL: http://www.reforma.com/interfase/articulo/555/1109131/ [Consulta 17 de mayo de 2010].

publicación de material personal, operaciones bancarias, pagos, compra-venta, entre otras.

Internet ha supuesto una revolución tecnológica como lo sostienen algunos autores. En el tema de las operaciones bancarias, estas permiten a los usuarios tener un mayor control de su información financiera y consultar con una mayor prontitud las operaciones que realiza en su cuenta.

Pensemos en el tiempo que nos llevaba esperar en el banco para poder realizar transacciones; los riesgos que se corrían por portar grandes cantidades de dinero en efectivo. Es por ello que se puede pensar como toda una revolución tecnológica la entrada de la banca en línea.

Instituciones como el Banco de México, así como, la Comisión Bancaria y de Valores considera que Internet es un medio alternativo al manejo de efectivo, sobre todo por el registro que se lleva de la procedencia de los recursos y los destinos.

El paso del dinero por Internet deja huellas que son registrables. Por ello la apuesta de las instituciones bancarias han apostado por reforzar la seguridad en los procesos, como es el caso del SPEI; y es aquí donde el usuario también tiene parte del control.

LA CONFIANZA DEL USUARIO EN LA RED

¿Confía usted en Internet? La confianza en Internet, plantea Jesús Vázquez Gómez, se fundamenta, principalmente, en el conocimiento que se tenga, las credenciales electrónicas que presente, por ejemplo, el logo, los sistemas de seguridad; o bien, de

lo que nos dice de ella un conocido.[89] Tal vez la confianza se genera del aval que respalde la operación, por ejemplo, las instancias de gobierno.

Como hemos visto anteriormente, parte de la desconfianza en realizar operaciones, ya sea de transferencias bancarias o de compra-venta por Internet, se debe al desconocimiento del sistema. De acuerdo con Marcus J. Ranum aunque exista una gran variedad de productos en el mercado relacionados con la seguridad, así como fabricantes, "pero estos productos y estos fabricantes no podrán ayudarle, a menos que comprenda lo que realmente hacen".[90]

Los usuarios no tienen que ser expertos informáticos, pues no todos tienen la posibilidad de conocer el funcionamiento de sus máquinas, incluso, muchos utilizan la computadora como herramienta para algunas actividades. Incluso desconocen cuan vulnerables son y se sorprenden cuando lo descubren.

Lo más preocupante es que se dan cuenta de ello demasiado tarde, ya cuando han sido víctimas de algún intruso. Lo más grave del asunto radica en que el usuario a veces no da importancia a estas intrusiones, o bien no sabe a dónde dirigirse. En el caso de los servicios como la banca en línea, muchas veces depende de la institución bancaria y el usuario se encuentra atado de manos, pero es aquí dónde tenemos que responsabilizarnos de la prevención.

LOS PRIMEROS PASOS PARA UNA NAVEGACIÓN SEGURA

¿Alguna vez ha escuchado la frase: "te vas con cuidado"? Generalmente es lo que se dice cuando una persona emprende un viaje, corto o largo, cuando vamos a la escuela o cuando salimos a un viaje mucho más lejano. En esa pequeña frase

[89] Octavio Islas; Claudia Benassini, *Internet, columna vertebral de la sociedad de la información,* México, ED Porrúa, Colección Humanidades TEC, 2005. P. 357.
[90] Stuart McClure, Joel Scambray y George Kurtz, Hackers: Secretos y soluciones para la seguridad de redes, España, Osborne McGraw Hill, Biblioteca Profesional, 2000, p. xxiv.

encontraremos los buenos deseos de la gente que nos aprecia y que espera tengamos una buena salida y un buen regreso. Pero va más allá de eso: implica que andemos con precaución y en alerta, fijarnos por dónde andamos, no andar por lugares solitarios, etcétera. Es así, como nos anticipamos a situaciones y tomamos las medidas de prevención para evitar un trago amargo.

Lo mismo ocurre en el caso de la seguridad en los portales bancarios, y de cualquier otro giro. Primero hay que conocer, anticiparse a lo que pudiera ocurrir y actuar en consecuencia. Hemos encontrado que entre los principales riesgos que corren los usuarios al momento de navegar en los portales bancarios o cuando realizamos alguna compra por Internet, lo que está en riesgo es la información, por lo que se puede hacer con ella: Modificación, copia, destrucción, conocimiento, provocación de pérdida (Ivonne Muñoz, 2009).

Lo anterior deriva en una serie de situaciones que ponen en riesgo la información confidencial del usuario, que puede derivar en un ilícito como: el robo de Identidad o de información, la suplantación de identidad, que puede derivar en la utilización ilícita de recursos o valores; el acceso ilícito a equipos y medios electrónicos del sistema bancario, que se relaciona con la clonación de instrumentos de crédito y pago (*skimming*); la destrucción de información crediticia; el repudio o denegación de un servicio.

El usuario es, entonces, un factor determinante en cuanto a seguridad se refiere. Si un banco no establece las indicaciones de manera clara y le advierte sobre los riesgos que corre al aventurarse a páginas de dudosa autenticidad, entonces el usuario podría estar incurriendo en un error que lo perjudique.

¿Pero cómo podemos evita caer en esas situaciones?

Las instituciones bancarias han puesto un especial énfasis en proporcionar las herramientas y los elementos que permitan al usuario un nivel de seguridad óptimo. En general, se siguen utilizando los sistemas de contraseñas para comprobar la identidad de los usuarios, esto es especialmente útil por lo relativamente sencillo que resulta proteger toda la información bajo el resguardo de una llave. Pero para evitar situaciones en el caso de los sistemas basados en contraseñas, se recomienda a los usuarios.[91]

- Mezclar mayúsculas, minúsculas y caracteres no alfabéticos.
- Longitud mínima de 6 caracteres.
- No usar palabras de diccionarios, ni con sentido, ni nombres propios.
- No utiliza únicamente números.
- No compartirla con nadie, ni escribirla en ningún sitio y que sea fácil de recordar.
- No utilice números de identificaciones como: su número de teléfono, ni matrículas, o cumpleaños. O bien, si llega a utilizarlos, procure intercalar con signos que no tengan nada que ver con estas fechas, es decir, el *password* no debe ser evidente.
- Cambiarla con regularidad.
- No usar una contraseña para todo.
- No utilice dos caracteres idénticos juntos.

Es importante señalar que encontrará el usuario algunas variantes en los sitios que utilizan este medio para corroborar la identidad de los usuarios. Encontrará algunas

[91] José Luis González, *op. cit., p. 398*

variantes, sobre todo en la cantidad de caracteres, o en que algunos indicarán que utilice otro tipo de caracteres además de los alfanuméricos. Pero pese a dichas variantes, debe ser consciente de que la contraseña no debe ser información evidente o que pueda ser revelada con facilidad.

Otra consideración importante es no dejar sesiones abiertas en los equipos que estamos utilizados, sobre todo si no son para uso exclusivo del usuario. Algunas personas confían en que una vez que cerraron la ventana de exploración, en automático se cierra todo lo demás. Para nuestro infortunio esto no ocurre siempre. Es como dejar la puerta parcialmente abierta. Un dicho conocido es el que reza: “La ocasión hace al ladrón”, y en este caso no demos esa oportunidad.

Una recomendación que sin duda debe ser considerada de cajón es la instalación de un antivirus y su constante actualización. Proteger los equipos personales es como la protección de su casa, coloca usted candados que dificulten la entrada de cualquier ladrón, pero si no se anticipa a los posibles ataques manteniéndose informado de lo nuevo en las modalidades del crimen, de nada le servirá su antivirus.

Evite guardar sus contraseñas en el equipo. Algunos usuarios, sobre todo tratándose de equipos portátiles o personales, suelen guardar las contraseñas con la finalidad de no ingresar a las aplicaciones cada vez que abre su sesión. Esto, al parecer facilitar en tiempo. No obstante, no siempre resulta una buena idea, en especial si su equipo lo comparte con alguien más.

LAS FIRMAS DIGITALES

Las firmas digitales son otra forma de garantizar que nadie usurpe nuestra identidad. Se utilizan generalmente al momento de realizar alguna compra, o trámite (como la facturación electrónica). Es otra forma que tenemos para corroborar nuestra identidad en Internet y evitar la suplantación. La firma electrónica es una serie de

caracteres que identifican a un signatario, es única, está avalada por una institución, que es la que valida dicha firma. El usuario tiene el control del uso de esta firma electrónica.

Actualmente, instituciones como el Sistema de Administración Tributaria apuesta por la firma digital, sobre todo cuando se trata de la facturación. “El objetivo del servicio de firma digital es asegurar la no existencia entre el emisor y el receptor”[92].

¿Cómo funciona? Se envía un mensaje y dentro de éste se deja una huella dactilar (la firma electrónica) la cual debe ser verificada por la institución. La firma electrónica tiene la misma validez que una firma manuscrita, al utilizarla el usuario certifica que él está autorizando dicha operación.

La firma digital, plantea Puentes Calvo, es una técnica que nos permite identificar al sujeto emisor al ligarlo mediante un código único. La confianza en este sistema se fundamenta en la certificación que hace otra institución y que valida la identidad. Es decir, se genera una serie de códigos que identifica al usuario frente a una instancia, sólo él puede hacer uso de esa firma, para lo cual genera una contraseña. La instancia tiene la obligación de validar esta información y confirmarla. Por lo que no cualquiera puede hacer uso de la firma única del usuario.

IDENTIFICACIÓN Y CERTIFICADOS DIGITALES

Al tratar este tema debemos hablar de la identificación y certificados digitales, que viene implícito en el tema de la seguridad. “La identificación crea responsabilidad y confianza”[93] de acuerdo con Juan Francisco Puentes Calvo. Sin duda, cuando nuestra identidad está respaldada por una institución bancaria, o bien, por un gobierno, o cualquier otro organismo con la competencia para avalarla, generamos

[92] Juan Francisco Puentes Calvo, *op. cit.* p. 96.
[93] *Ibid,* p. 100.

confianza. Particularmente cuando se trata de realizar trámites u operaciones que requieren de una identificación real, que corresponda con nosotros.

Hay dos tipos de identificación: una basada en algo que se sabe (nombre de usuario y *password*); y otra fundamentada en algo que se tiene, como las tarjetas de identidad, o bien las firmas digitales. En este caso los usuarios garantizan que son ellos y no alguien más quien realiza la operación, generando un estado de confianza entre el emisor y la institución receptora.

Un certificado digital es la versión electrónica de una identificación, algo parecido a la credencial de elector. Esta identificación es única. La certificación digital funciona para los usuarios que desean realizar transacciones bancarias, como el ya mencionado SPEI, comercio electrónico, o bien, trámites gubernamentales.

En México, por ejemplo, se utilizan este tipo de certificados en la Secretaría de Hacienda. Ahora puede usted realizar las declaraciones de impuestos vía Internet, siempre y cuando genere un certificado o firma digital. Esto, sin duda, facilita ciertos trámites que anteriormente requerían de mucho tiempo. La firma digital, en este ejemplo, la genera la misma instancia gubernamental. No obstante aún no contamos con la infraestructura necesaria para general identificaciones universales para todos los trámites.

EVITEMOS EL FRAUDE. EL USUARIO AL SERVICIO DEL USUARIO.

Hemos repasado algunas formas de fraude a las que podemos estar expuestos como el *pharming* y el *phishing*. Ambos son un ataque directo a la seguridad de los clientes. Ahora nos enfocaremos en proporcionar algunas recomendaciones generales que disminuyan considerablemente los riesgos de ser víctimas de estos fraudes.

Sabemos, como ya se explicó en el capítulo II, que el *phishing* y el *pharming* operaban generalmente a través del correo electrónico. El usuario recibía un mensaje con una liga que, aparentemente, era de un banco u otra institución, o bien, de alguna que parecía oficial. Después solicitaban información como la contraseña u otros datos personales (sin que el usuario note que es una página fraudulenta[94], pues clonan perfectamente el diseño de los portales). "Por esta razón se les recomienda sospechar de cualquier correo electrónico que solicite información personal"[95], mucho más dudoso cuando se argumente problemas técnicos o confirmación de información, o bien, premios, entre otros.

"No proporcionar información personal como contraseñas, nombre de usuario". Esto sobre todo cuando se solicitan vía correo electrónico. Una de las advertencias de los bancos es justo ese, que el banco, bajo ninguna circunstancia solicitará información vía correo electrónico. Lo mismo ocurre con otros sitios, así que si usted recibe una invitación de este tipo, simplemente ignórela y envíela directo al bote de basura virtual.

"Antes de proporcionar cualquier dato sensible como cuentas bancarias, números de tarjeta de crédito o contraseñas, asegúrese de que se encuentra en el sitio oficial y no en una redirección". Es decir, si le aparece una liga (de nuevo) mediante correo electrónico, desconfíe y verifique. Cheque si los portales que visiten emplean un protocolo seguro como https en lugar de un http. Habrá que explicar que estos se encuentran al inicio de la dirección URL. "Revisar frecuentemente el archivo *host*. Este archivo contiene registros de traducción de nombre de dominio a dirección IP y eliminar"[96].

"No emplear permisos de administrador para tareas cotidianas que no requieran dicho privilegio, esto evitará que algún código malicioso pueda modificar el archivo

[94] Miriam J. Padilla Espinosa, *ibid.*
[95] *ibid.*
[96] Juan Patiño Corona, *ibid.*

host, o cualquier otro archivo del sistema"[97]. Y una última recomendación, no por ser menos importante, se debe denunciar cualquier incidente. En caso de que nos encontremos en una situación de fraude, el primer paso es reportarlo inmediatamente a la institución bancaria.

Es importante, para levantar un reporte, proporcionar información importante por lo que conviene que el usuario tenga a la mano datos como: el número de la cuenta afectada y tener los documentos oficiales que avalen nuestra identidad y las especificaciones del delito cometido como: posibles accesos no autorizados a nuestras cuentas, movimientos irregulares, cargos no autorizados, pérdida de contraseña, perdida de *token* (es un dispositivo que proporciona el banco con una serie de contraseñas desechables, para realizar operaciones bancarias electrónicas).

UN VOTO DE CONFIANZA A LA BANCA EN LÍNEA

Se dice que el desconocimiento genera incertidumbre. Desconocer el funcionamiento de algún procedimiento, nos puede impedir aprovechar al máximo las ventajas que nos puede proporcionar. Internet es un gran avance para la sociedad, un ejemplo claro es la banca en línea.

El avance de la tecnología es tan veloz y vertiginoso, que no nos ha dado tiempo de reflexionar en temas como la seguridad. Y en el caso de Internet, se ha perfeccionado sobre la marcha. Los errores que en algún momento fueron minando la confianza de los usuarios se han corregido poco a poco, pero lo cierto es que no es un trabajo terminado aún. Tanto el Estado, como las instituciones bancarias y los usuarios tendrán que trabajar en establecer un camino en el que la confianza de los usuarios esté blindada.

[97] Juan Patiño Corona, *ibid.*

Conclusiones

Al concluir este trabajo se pueden generar una serie de reflexiones en torno al tema de la seguridad en Internet y al cómo se aborda desde el periodismo. Se trata de un tema complejo y que hasta la fecha se ha tratado más en el ámbito especializado. Una de las primeras dificultades a las que me enfrenté fue a la delimitación del tema, sabemos que para poder realizar esta fase de la investigación es importante contar con algunas lecturas previas, o con algún conocimiento general del tema.

En este caso, aunque contaba con una idea de lo que quería, conforme avanzó la investigación, me di cuenta que el tema era mucho más amplio de lo que me imaginaba y que tocaba más aristas de las que planteaba en un inicio. Pese a esta primera dificultad, logré definir conforme marchaba la investigación mi foco de estudio, pero se sugiere a quienes pretendan incursionar en esta temática acercarse a los que conocen del tema para que les ayude a definir mejor.

Otra dificultad que se planteó lo relacionado a los conceptos. Al momento de revisar las fuentes, me percaté de que muchas veces no manejamos los términos de la manera correcta. Generalmente usamos palabras de manera cotidiana como: *hacker*, *SPAM*, virus, gusanos, *hacking*, entre otros, pero a estas definiciones no siempre las aplicamos correctamente, o bien, se modifican. Por ejemplo, durante la entrevista al experto Roberto Sánchez Soledad aclaró que ya se utiliza *Malware* para todo lo relacionado con gusanos y virus.

Los términos en materia de tecnología no son definitivos, como en el caso de los *hackers*, porque se van definiendo de acuerdo a sus objetivos y a sus funciones. Incluso la misma comunidad de hackers están trabajando para delimitar quién es quién. Es por ello que podemos encontrar personas que se dedican a identificar debilidades en los sistemas de seguridad.

Es posible explicar al usuario términos que no son de uso común, pero aquí el esfuerzo del periodista tiene que duplicarse. En algunos casos es posible dejar a un lado dichos términos, siempre y cuando no pierda sentido el reportaje. Para ello debemos revisar con detenimiento cuáles conceptos son necesarios y de cuáles podemos prescindir.

Un hacker no es un delincuente. Hemos encontrado que lo que une a esta comunidad es la pasión por el conocimiento, por imponerse retos constantemente, el desafío intelectual es lo que los motiva. Aunque el para qué lo hacen, es lo que determina si es con fines maliciosos o no. De esto ya se han percatado las empresas y contratan a este tipo de personas para reforzar sus sistemas de seguridad.

En el transcurso de este trabajo, me percaté de la importancia de ir de la mano de un experto, es la mejor forma de trabajar con temas de ciencia y tecnología; pero también me enfrenté a la necesidad de capacitarme mejor en este tema. Esto facilita la búsqueda de información y la interpretación de los datos obtenidos.

Respecto al tema podemos concluir que:

1. El uso de Internet forma parte de la vida cotidiana, quien no maneje la computadora y el Internet en lo más básico, es una persona desactualizada, incluso, se habla del analfabetismo informático. La tendencia es que se convierta en una habilidad básica para las generaciones presentes y futuras. Como un dato extra, en algunas escuelas primarias se imparten como materias extracurriculares: inglés y computación. No es materia para esta investigación, pero es un dato que puede dar pie a otro proyecto.

2. El uso que se les da a las nuevas tecnologías es una preocupación latente. Se encontró que así como nos facilita las operaciones bancarias,

también encontramos que la seguridad es un aspecto que debemos cuidar generando una cultura, en el que se fomenten las buenas prácticas de los usuarios para proteger su información personal. Esto nos lleva a la siguiente conclusión:

3. Se tiene que fomentar una cultura en seguridad entre los usuarios. Aún nos encontramos con personas que ingresan información confidencial sin ninguna precaución en los cafés Internet; o que no deshabilita la opción de guardar contraseñas en estos lugares públicos. También vemos un rechazo a "gastar" en un *software* original, muchos prefieren pagar menos, pero no se dan cuenta de que a largo plazo puede tener mayores costos.

4. En el ámbito de las instituciones bancarias y de los servicios de banca en línea, se debe enfatizar en las buenas prácticas de seguridad ya tratadas en el capítulo III. Asimismo se debe orientar a los usuarios en los temas del fraude electrónico. Los bancos deben trabajar constantemente en la seguridad de la información de los usuarios, pero también ofrecer información clara y puntual de cómo utilizar sus servicios en línea. La responsabilidad es compartida, entre el la institución que proporciona el servicio y la capacitación del usuario.

5. Debemos entender que no todos los usuarios conocen el funcionamiento de las transferencias electrónicas o el comercio electrónico. Se debe pensar en un usuario promedio al momento de ofrecer los servicios de banca electrónica e información básica para que sus operaciones sean seguras. Los errores que a veces se cometen y que derivan en fraudes se deben a desconocimiento, pues mucha ocasiones el usuario no sabe como generar contraseñas seguras o es víctima de correos fraudulentos.

6. México cuenta con un marco legal aplicable, si bien no se trata de una ley general y específica para el tema informático, sí tiene apartados específicos en otras leyes, como modalidades. Encontré que la manera más práctica y rápida para desarrollar defensas en contra de los ataques que van surgiendo a nivel internacional, es a través de los foros internacionales.

La actualización y el surgimiento de nuevas tecnologías no permite hablar de un tema acabado. Seguramente al cerrar esta tesis algo se habrá actualizado en cuanto a seguridad, pero lo importante es no perder de vista que es necesario trabajar en una cultura en los usuarios en materia de seguridad, pues no existe un sistema cien por ciento seguro, pero sí pueden generarse buenas prácticas en seguridad que disminuyan los riesgos de tener un sistema vulnerable.

Bibliografía

1. Pedro A. Miguel Asensio, *Derecho del comercio electrónico*, México, Ed Porrúa, 2005, 336 pp.

2. Asa Brigs; Peter Burke, *De Gutenberg a Internet. Una historia social de los medios de comunicación*, México, Ed Taurus, 2006, 425 pp.

3. Enrique Bustamante (coord.), *Comunicación y cultura en la Era Digital. Industrias, mercados y diversidad en España*, España, Ed Gedisa, 2002, 382 pp.

4. Edeliberto Cifuentes Medina, *La aventura de investigar: el plan y la tesis*, Guatemala, Ed Magna Terra, 2005, 2a ed, 213 pp.

5. Umberto Eco, Cómo se hace una tesis: técnicas y procedimientos de estudio, investigación y escritura, México, Ed Gedisa Mexicana, 2004, 232 pp.

6. Urs E. Gattiker, *The information Security Dictionary: Defining the Terms that Define Security for E-Bussines, Internet, Information and Wireless Technology*, EUA, Kluwer Academic Publishers, 2004, 411 pp.

7. José Luis González S.; Marisol Sánchez A; Alfonso Gazo C., *Autopistas de la Información e Internet: Tecnología, Servicios, Peajes y Normas de Navegación*, Universidad de Extremadura servicio de publicaciones, 1998, 456 pp.

8. Luis Alberto Hernando Cuadrado, *El discurso periodístico*, Madrid, Ed Verbum, Colección Cervantes, 119 pp.

9. Octavio Islas; Claudia Benassini, *Internet, columna vertebral de la sociedad de la información,* México, ED Porrúa, Colección Humanidades TEC, 2005. 400 pp.

10. Charles Jennings; Lori Fena, *La Centésima ventana: guía para proteger la seguridad y privacidad en la era de Internet*, España, Ed Deusto, 2000, 221 pp.

11. Alberto R. Lardent, *Sistemas de información para la gestión empresaria: Planeamiento, Tecnología y Calidad*, Buenos Aires, Pearson Education, 2001, 523 pp.

12. Stuart McClure, Joel Scambray y George Kurtz, *Hackers*: Secretos y soluciones para la seguridad de redes, España, Osborne McGraw Hill, Biblioteca Profesional, 2000, 514 pp.

13. Lev Manovich, *El lenguaje de los nuevos medios de comunicación. La imagen en la era digital*, España, Ed Paidós Ibérica, Colección: Paidós Comunicación 163, 2005. 431 pp.

14. Ana María Menéndez Marcín, *Estrategias para elaborar libros: Metodología para citas y referencias bibliográficas*, México, Ed. Porrrúa, 2006, 115 pp.

15. Salvador Mercado H., *¿Cómo hacer una tesis?: licenciatura, maestría y doctorado*, México, Ed Limusa, 2008, 4a ed., 375 pp.

16. Santiago Muñoz Machado, *La regulación de la red: Poder y Derecho en Internet*, España, Ed Taurus, 2000. 288 pp.

17. Ivonne Muñoz Torres, *Delitos informáticos: Diez años después*, México, Ed Ubijus, 2009. 248 pp.

18. Juan Francisco Puentes Calvo, *Principios de seguridad en el comercio electrónico,* México, Ed Alfaomega Ra-Ma, colección Navegar en Internet, 2009, 256 pp.

19. Toby J. Velte, *Fundamentos de comercio electrónico*, México, Ed McGraw-Hill, serie Biblioteca Profesional, 2001. 486 pp.

20. Óscar Zapata A., *La aventura del pensamiento crítico: herramientas para elaborar tesis e investigaciones socioeducativas*, México, Ed Pax, 2005, 295 pp.

Hemerografía

1. Ximena Gutiérrez Velázquez, “Los *hackers*: en los límites de lo posible”, Revista ¿cómo ves?, Año 12, Núm. 138, México, UNAM/DGDC, mayo, 2010.

Referencias Electrónicas

2. David Alandete, “Una red roba datos clave de 74.000 ordenadores en el mundo”, [en línea], España, El País.com, 19 de febrero de2010, Dirección URL: http://www.elpais.com/articulo/sociedad/red/roba/datos/clave/74000/ordenador

es/mundo/elpepisoc/20100219elpepisoc_2/Tes [consulta: 14 de mayo de 2010]

3. David Brooks, “Grandes bancos de EU aceptan lavar narcofondos mexicanos”, [en línea], La Jornada On Line, México, 30 de junio de 2010, Dirección URL: http://www.jornada.unam.mx/2010/06/30/index.php?section=economia&article=025n1eco [Consulta: 20 de Septiembre de 2010]

4. Jordi Buch i Tarrats y Francisco Jordan, *La Seguridad de las transacciones bancarias en Internet*, [en línea] Pamplona, Sociedad Española de Informática de la Salud, 2001. Dirección URL: http://www.conganat.org/seis/informes/2001/PDF/6BuchTarrats.pdf, [Consulta: 10 de mayo de 2010]

5. Estudio AMIPCI, *Hábitos de los Usuarios de los usuarios de Internet en México: Resumen Ejecutivo,* [PDF, online], México, Asociación Mexicana de Internet, Mayo 2009, Dirección URL: http://www.amipci.org.mx/estudios/temp/RESUMENEJECUTIVOEstudioAMIPCI2009UsuariosdeinternetFINAL-03347250012456912 60OB.pdf, [Consulta: 10 de mayo de 2010]

6. *Estudio AMIPCI de Banca por Internet en México 2007. Resumen Ejecutivo*, [en línea], México, Asociación Mexicana de Internet, 2007, Dirección URL: http://amipci.org.mx/estudios/temp/EstudioAMIPCIdeBancaporInternetenMexico2007RESUMENEJECUTIVO-095394800120352190 3OB.pdf [Consulta: 1 Junio de 2010]

7. Europa Press, “Detenidas siete personas por fraude mediante ‘*phishing*”, [en línea], España, El País.com, 8 de abril de 2010, Dirección URL: http://www.elpais.com/articulo/tecnologia/Detenidas/personas/fraude/mediante/phishing/elpeputec/20100408elpeputec_6/Tes, [Consulta: 14 de mayo de 2010]

8. Gobierno Federal, SEGOB, SHCP, SSP, PGR, Estrategia Nacional para la Prevención y el Combate al Lavado de Dinero y el Financiamiento al Terrorismo, Gobierno Federal, México, http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/814619//archivo [Consulta: 20 de septiembre de 2010].

9. *Informe Trimestral (Enero-Marzo 2004)*, [en línea, PDF], México, Procuraduría General de la República, Dirección URL: http://www.pgr.gob.mx/temas%20relevantes/Documentos/Informes%20Institucionales/1trimestre2004.pdf [Consulta: 28 de mayo de 2010]

10. Tania M. Moreno. “Las 5 caras del lavado de dinero”, [en línea], CNN Expansión, Ciudad de México, martes 08 de junio de 2010, Dirección URL: http://www.cnnexpansion.com/economia/2010/06/07/lavado-de-dinero-narco-mexico-eu [Consulta: 25 de octubre de 2010].

11. Alberto Nájar. “Nuevas reglas contra el lavado de dinero en México”, [en línea], BBC Mundo, México, última actualización: martes 15 de junio de 2010, Dirección URL: http://www.bbc.co.uk/mundo/economia/2010/06/100615_2119_mexico_lavado_dolares_gz.shtml [Consulta: 06 de agosto de 2010]

12. Juan Patiño Corona, “*Pharming*, la evolución de un Ataque”, [en línea], México, Punto Seguridad-Defensa Digital, UNAM, Número 2, Agosto 2009, Dirección URL http://revista.seguridad.unam.mx/rs_unam_02/001_03/art_03.html [Consulta: 03 de mayo de 2010]

13. Miriam J. Padilla Espinosa, “Pescando Información *Phishing*”, [en línea], México, Punto Seguridad-Defensa Digital, UNAM, Número 2, Agosto 2009, Dirección URL: http://revista.seguridad.unam.mx/rs_unam_02/001_02/art_02.html [Consulta: 03 de mayo de 2010]

14. Notimex, “Ampliará bancos servicio electrónico”, [en línea], México, El Universal.com.mx, 24 de mayo de 2010, Dirección URL: http://www.eluniversal.com.mx/notas/682655.html [consulta: 24 de mayo de 2010].

15. Notimex, “CNBV apoya disminuir uso de efectivo”, [en línea], México, El Universal.com.mx, 24 de mayo de 2010, Dirección URL: http://www.eluniversal.com.mx/notas/682688.html [consulta: 24 de mayo de 2010].

16. Elena Pérez Gómez, ¿Qué es la informática forense o Forensic?, [en línea], España, MICROSOFT, Centro para Empresas y Profesionales, Dirección URL: http://www.microsoft.com/business/smb/es-es/legal/forensic.mspx [Consulta: 30 de julio de 2010].

17. Justin Pierce, *World Internet Project Report finds large percentages of Non-users, and significant gendre disparities in going on line*, [on line, PDF], USC ANNENBERG School for Communication & Journalism, 26 de febrero de 2010, Dirección URL: http://www.worldinternetproject.net/

18. Procuraduría General de la República, *El gobierno mexicano combate a fondo la explotación sexual infantil,* [en línea], México, Boletín no. 132, 10 de febrero

de 2004, Dirección URL: http://www.pgr.gob.mx/cmsocial/bol04/feb/b13204.htm [consulta: 28 de mayo de 2010]

19. Real Academia Española, www.rae.es

20. Secretaría de Seguridad Pública, PFP, *Prioritario endurecer e intensificar acciones para disuadir delitos cibernéticos; DC México*, [en línea], Boletín electrónico 329/03, México, 19 de mayo de 2003, Dirección URL: http://www.ssp.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_pageLabel=sspN_page_3&nodeId=/BEA%20Repository/95782//archivo&pathImg=%2FBEA+Repository%2Fimport%2FIndices+de+Transparencia%2FLey+de+Transparencia+en+la+SSP%2FContenidos+de+Boletines%2FBoletines+de+Octubre%2FBolet%C3%ADn+N%C3%BAmero+329&docName=Secretar%C3%ADa%20de%20Seguridad%20P%C3%BAblica [consulta: 3 de mayo de 2010]

21. *s/a, Gestión de Riesgos para la banca electrónica y actividades con dinero electrónico* [PDF, en línea], Brasilea, Comité de Brasilea para la Supervisión Bancaria, marzo de 1998, Dirección URL: http://www.asbaweb.org/documentos/publicaciones/98-PUB-ESP-gestion%20de%20Riesgos%20para%20la%20Banca%20electronica.pdf [25 de mayo de 2010]

22. s/a, s/t, [online], España, Real Academia Española, Ed Espasa Calpe, 2008, 23.ª edición, Dirección URL: http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=internet, [Consulta: 5 de mayo de 2010]

23. s/a, "Avanza banca electrónica en México", [en línea], México, ElUniversal.com.mx, 10 de abril de 2009, Dirección URL: http://www.eluniversal.com.mx/articulos/53468.html [consulta: 24 de mayo de 2010]

24. s/a, "14 detenidos por robar datos bancarios en Internet", [en línea], España, El País.com, 29 de junio de 2009, Dirección URL: http://www.elpais.com/articulo/sociedad/detenidos/robar/datos/bancarios/Internet/elpepusoc/20090629elpepusoc_4/Tes [Consulta: 14 de mayo de 2010]

25. Aida Ulloa, "Día de Internet", [en línea], México, El Universal.com, 14 de mayo de 2007, Dirección URL: http://www.eluniversal.com.mx/finanzas/57755.html [Consulta: 10 de junio de 2010]

26. Verónica Valencia, “Crece internautas 11% desde 2008”, [en línea], Distrito Federal, Reforma.com, 17 de mayo de 2010, Dirección URL: http://www.reforma.com/interfase/articulo/555/1109131/ [Consulta 17 de mayo de 2010].

Entrevista

M. en C. Roberto Sánchez Soledad. Jefe del área "Atención a incidentes" de la Subdirección de Seguridad de la Información/UNAM-CERT. Lunes 11 de octubre de 2010.