Delito Electrónico

Compilación

© Sahnya Shulterbrandt
Lic. Genaro D. Salom
Lic. Valentín Arteaga

¿Cuál es la verdad sobre seguridades de Internet y los usuarios?

La mayoría de los usuarios del Internet no están concientes de los riesgos y falta de seguridad a los que estamos expuestos cuando nos conectamos. Sólo un pequeño grupo lo está. Incluso un gran número de empresas carece de políticas y regulaciones por escrito para que sus empleados utilicen los sistemas y el Internet correcta y éticamente.

El Comité para el Desarrollo del Comercio de la Organización Mundial del Comercio (OMC) celebró el pasado mes de abril un seminario sobre las implicaciones de los ingresos del comercio electrónico. Además de analizar las estadísticas del crecimiento del e-Commerce, su reciente desarrollo y sus implicaciones futuras, algunos de los expositores y participantes reflexionaron sobre la necesidad de **regulaciones universales** en este ámbito.

El tema también esta siendo discutido en otras instancias. En el marco de las negociaciones del Acuerdo de Libre Comercio para las Américas, el famoso ALCA, se ha integrado el denominado "Grupo Especial sobre Comercio Electrónico" (ECOM). **Resulta curioso el caso de algunos países, donde las Comisiones Nacionales solo esta integrada por representantes de las compañías proveedoras de servicios de telecomunicaciones.**

Pero las iniciativas y preocupantes sobre estos aspectos no es nada nuevo, ni reciente. Ya en el año 2000, en la reunión de los G-8, en Paris, una comisión especial participó en un diálogo entre la Industria y el Gobierno sobre "Seguridad y Confianza en el Ciberespacio". Desde mucho antes la confianza de los usuarios se había visto amenazada por las crisis de virus.

Es de todos sabido que las empresas lideres en el mercado utilizan el Internet como herramienta de productividad. Superado el denominado período experimental (1995-2000) en el que la Web era un elemento separado del negocio e iniciado el denominado período de uso racionalizado (2000-2003) en el que la Net se utiliza como canal integrado, se nos hace claro como el **atentar contra su uso es un crimen de dimensiones inimaginables.**

Según estimaciones de la Forrest, en los próximos años habrá un incremento de 15% en las ganancias del e-business. Entonces, cuando un virus se adueña del ciber espacio se da el fenómeno que en reiteradas ocasiones se ha denominado de "estados de histeria" por parte de los usuarios. De allí que igualmente se ha hablado sobre cibercrimen y ciberterrorismo, ya que estas acciones de virus e intrusiones atentan contra el comercio y pueden desbastar una empresa en un lapso sumamente corto de tiempo, llevándola incluso a la quiebra.

¿Recuerda usted los casos de amtrax en el correo de los EE.UU.? Eso fue considerado como un crimen, verdad? Lo mismo pasa respecto a los virus

electrónicos que atentan contra el usuario, las empresas, los gobiernos y las operaciones electrónicas.

Usted, de seguro, no esta exento de estas afirmaciones y de este proceso. Si quiere hacer una rápida prueba piense si ha variado su presupuesto en tecnología con respecto al año pasado? Por favor, piense también cuánto podrá cambiar para el año 2005? Por último considere por un segundo qué nuevas innovaciones conducirán el comercio en el 2010?

Ahora recapacite, en sus transacciones ha sustituido el uso del teléfono y del fax. Que las ordenes de pedido de sus clientes y las solicitudes de cotizaciones de los potenciales consumidores llegan por Internet. Que por esa misma vía usted solicita a sus suplidores con un mínimo de gastos todo el material gastable de su negocio, su mercadeo es a través del Internet. Realiza sus pagos por transferencias automatizadas y hace sus declaraciones impuestales y pagos por un servicio de e-Procurement del Gobierno de su ciudad.

Entonces un buen día han hackeado su sistema. Alguien se adueño de sus claves y ha hecho de las suyas. Su Web Site en lugar de vender los productos que con tanto esfuerzo ha creado, ofrece servicios pornográficos. En ese momento, ¿puede usted decirme a quien se va a dirigir? **¿Pudiera decirme si los famosos SpamCOPS podrán hacer algo para ayudarlo?**

Hace unos años el Sitio Web de una de las cumbres presidenciales fue hackeado y convertido en vitrina pornográfica. Recientemente el Web Site de la UNIFEM, agencia de las Naciones Unidas, igualmente fue victima de otro delito similar. Constantemente recibimos virus en nuestras bandejas de entrada de correos. **Esta semana, solamente, hemos recibido más de 700 correos con virus.**

Nuestros sistemas de seguridad nos muestran en sus record como una y otra vez personas inescrupulosas tratan de violentar la privacidad de nuestros sistemas y hemos podido constatar como nuestros correos son interceptados y leídos, antes de llegar a nosotros. **Algunos simplemente no llegan.**

Tal es la situación en el ciber-espacio (podríamos llamarle ciber-oeste) que hemos recibido testimonios sobre prácticas de empresas que en el afán conquistar nuevos usuarios de la competencia han abrumado a sus clientes con virus. Y de otras cuyos empleados pasan el tiempo leyendo la correspondencia privada de los consumidores.

En un seminario realizado el año pasado un asistente manifestó como un prestigioso periódico era usuario frecuente de Sites XXX (pornográfico). ¿**Qué dirán los directivos si se dieran cuenta de cómo se utiliza la conectividad que le ofrecen a sus periodistas y empleados?** ¿Esta usted seguro que el IP de su empresa no esta registrado en un sitio non-grato?

Se hace necesario que el sector privado y el gubernamental encaminen sus esfuerzos para la creación de un marco jurídico universal que regule las operaciones de la conectividad, pero también que sirva para que el delito electrónico sea juzgado como tal y las acciones de quienes violenten la privacidad sean sancionadas con el peso de la ley.

Es imprescindible la creación de un organismo universal, no nacional, Ciber Cortes de Justicia, como propone Malasia, que regulen internacionalmente las operaciones transnacionales, algo como la Corte Interamericana de Derechos Humanos o más amplio como la Corte Internacional de Justicia.

También se hace necesario un sistema judicial que se encargue de ejercer las correspondientes acciones de emplazamiento. **No como los "SpamCops" que no ofrecen ningún beneficio o seguridad, al usuario y al comercio. Muy al contrario, son una amenaza a las libertades; un detrimento al desarrollo y crecimiento del comercio electrónico; y en ocasiones entidades cuestionables.**

El Internet es un medio masivo de comunicación

- Imprescindible para el desarrollo económico global.
- Instrumento indispensable de "mercadeo libre"
- Un arma poderosa para asuntos políticos e influencias de los Estados
- Factor determinante en la evolución de la globalización
- Instrumento de "educación" en todas las áreas
- Homogenizador de culturas y líneas de pensamiento
- **Un símbolo sin igual de la verdadera democracia y libertad mundial**
- **Importante para el sano funcionamiento de los gobiernos (e-Government)**
- **Fuente noticiosa efectiva y completa**
- **Estrechamente ligado con la libertad de presa y libre expresión**

Los organismos que debieran regir estas problemáticas están haciendo muy poco para homogenizar las reglamentaciones, mejorar las situaciones de Hackers, Crackers, intrusiones, fraudes y demás.

No hay un organismo universal hoy día que rija las operaciones en red, desde ninguna perspectiva. Si hay, sin embargo, empresas de "SpamCOP", que con fines de lucro, operan como policías, pagado / subsidiado por grupos anti-spam. En la mayoría de los casos parcializados **¿cómo se financian estas instancias?**

Es vergonzoso que hoy día no se pueda llegar a un consenso general de qué es y cómo tratar los diferentes problemas que están presentes sin aparente acción por parte de quienes deben de aplicar las soluciones.

Compañías de intereses privados y de alta integridad como Symantec, Panda, McAfee, entre otras son las que nos brindan cierto nivel de seguridad **relativa** con los Softwares y algunos servicios gratuitos que suelen ofrecer como los boletines de alertas y los Scans On-Line.

Quisiéramos conocer algún "Crimecop" un "Crackercop". ¿Conoce usted alguno? Los virus y los otros delitos son de carácter intencional entonces los inservibles Spamcops tienen una incidencia cuestionable desde el ámbito comercial y desde el ámbito de la efectividad operativa. **Usted no reporta a la Policía una carta promocional que pueda llegarle por correo.** Entonces pongámosle

atención a las verdaderas infracciones y delitos cometidos. **"No se deben restringir las Libertades."**

Debemos todos los interesados en las nuevas tecnologías de la Información y Comunicación (NTIC) hacer un esfuerzo para eliminar a Crackers, Hackers y demás especies viruales. Procesar y exigir que los crímenes electrónicos sean juzgados. Perseguir y enjuiciar a las personas y entidades responsables de cualquier crimen electrónico. **Debemos de velar por la total y absoluta libertad en el medio incluyendo su contenido y el flujo de correspondencia comercial, política, social y personal.**

La cultura de vida basada en información, aprendizaje e innovación es la base del desarrollo. Los países empiezan a perder sus ventajas comparativas tradicionales en el aspecto económico en relación a otras sociedades.

Es irrefutable la necesidad de conducir las economías a más elevados niveles de productividad a través de la tecnología. Es imprescindible la adopción y aplicación de las NTIC's para crear la competitividad nacional y romper las brechas digitales y alcanzar el desarrollo. Pero creando estructuras que sean proactivas; no destructivas o que impliquen o incidan a detener el comercio electrónico y el libre flujo de la información.

Al no existir una regulación en muchos países y estar los sujetos de derecho en lugares diferentes, se hace difícil, muchas veces imposible el implementar resoluciones en asuntos internacionales. Por su propia naturaleza el e-Commerce exige que este sea regulado, se debe exigir un marco de políticas claras para crear un clima de crecimiento saludable y estable.

Ha quedado en manos de empresas privadas el regular las operaciones en Internet. Es como el cuento de las Compañías Privadas de Seguridad. Esta muy bien que se contraten estos servicios para un nivel de protección especial, pero el que la ciudadanía de una nación no tenga la confianza o seguridad del Sistema Policial es algo que deja mucho que pensar.

http://www.revistainterforum.com/espanol/articulos/050602tecno.html

Delito: Crimen Electrónico

Concepto.

Crimen Electrónico, Fraude Electrónico. Es todo acto que infringe la ley y que se realiza aplicando algún medio de procesamiento electrónico. Por ejemplo: El robo a un Banco, violando la seguridad de algún medio de procesamiento electrónico de información, es constituido de crimen electrónico.

No se considera Crimen Electrónico el que el mismo Banco sea robado utilizando como medio artefactos electrónicos de alta tecnología que permita la comisión del delito. Seria bueno recordar que todo delito necesita determinados elementos objetivos y subjetivos para su identificación y diferenciación de acuerdo al agente comisor, su modo de operar y los medios que utiliza en su acción.

Un ejemplo sencillo: El HURTO se diferencia de la ESTAFA porque en este último es imprescindible el elemento subjetivo: engaño, mientras en aquel no. Otro elemento diferenciador es que en el HURTO el bien se sustrae o se apoderan de él, mientras en la ESTAFA el bien se entrega tácita o expresamente.

Ahora con esta breve explicación de los elementos que integran un determinado delito y la diferencia reseñamos que en el caso de crimen electrónico debe estar presente el elemento utilizando medio de procesamiento electrónico entre otros.

Las estafas realizadas por telemercadeo no son consideradas crimen electrónico. En ellas aunque se utilizan instrumentos de tecnología electrónica (teléfono, radial, televisiva) carecen del elemento que lo tipifica ¿Cuál? El Procesamiento Electrónico. El robo a un cajero automático realizado por un ratero directamente al cajero, violando el artefacto físicamente, tampoco es considerado un crimen electrónico.

Sin embargo, una violación de la seguridad del cajero utilizando tarjetas falsas precodificadas, sí lo tipifica como tal porque viola la forma electrónica de la seguridad del cajero.

Las acciones que más tipifican el delito electrónico son:

- Espionaje de comunicaciones, clave de la mayoría de los delitos electrónicos;
- Interferencia de comunicaciones por vía telefónica utilizadas con más frecuencia en Fraudes con Tarjetas de Crédito, Chantajes, Espionaje Industrial, Espionaje entre países.

Los delitos más conocidos dentro de la familia delictiva denominada crimen electrónico son:

- Fraudes con tarjetas de crédito en las transferencias electrónicas principalmente de los denominados cajeros automáticos. Estos fraudes se comenten principalmente violando los sistemas de criptografía (PIN). Precedentes de este tipo de delito en Francia y Alemania, a principios de la década de los 90's donde se determino en una corte que la responsabilidad de este tipo de delito no debía recaer en el tarjeta habiente, sino en la seguridad criptográfica de la institución bancaria, identificándose las variantes de posibilidades alternar de identificar el PIN por diferentes métodos, reduciendo a menos de 350 las posibilidades de identificación;
- Estafas en los Procesos de Pagos On-Line en las transacciones comerciales, por violación de los códigos de seguridad, por robo de los números de tarjetas de crédito;
- Espionaje: Internacional, Industrial y Personal: Manipulación de la información, ya sea personal, comercial / industrial o nacional. Actualmente se debate intensamente sobre la Violación de la Privacidad Personal y la divulgación sin autorización de datos personales. Por Ejemplo: Como podría

utilizar una aseguradora los datos médicos de una persona para rechazar una solicitud de póliza.

Otros delitos frecuentes son:

- Problemas técnicos como el caso del fallo de un Firewall;
- Virus Electrónicos;
- Engaños o estafas por Correos Electrónicos, como las cadenas de envío.

Algunos Antecedentes: OPERACIÓN DIABLO DEL SOL

En el pasado cuando las tarjetas de crédito eran autorizadas de forma mecánica a través de llamadas telefónicas el delito se podía tipificar atendiendo a las siguientes características:

- Robando la tarjeta de otra persona y utilizándola como de su propiedad.
- Interfiriendo las llamadas de los centros de consumo asumiendo el papel del autorizador para realizar la autorización.

Estos modus operandi del pasado y que aún persisten en la actualidad por rateros vulgares no se consideran crimen electrónico ¿Por qué? Falta el elemento: Procesamiento Electrónico.

Con el desarrollo vertiginoso del mundo digital y el uso generalizado del Internet surgió esta modalidad delictiva a escala mundial y con más proliferación en los países desarrollados de forma que se necesitaría una policía cibernética mundial tan preparada y eficiente, como el FBI, y solamente en Gran Bretaña se esta creando este tipo de policía.

En 1990 en los EE.UU. en más de 10 Estados entre varias actividades anti-hacker, se realizo la denominada “Operación Diablo del Sol” que fue que recibió mayor difusión publica por las arrasadoras incautaciones de ordenadores en todo el territorio norteamericano sin precedentes en la historia.

La operación no se propuso combatir la actividad de HACKER en cuanto a intrusiones informáticas, como otras operaciones anteriores, sino más bien como un castigo severo al azote del bajo mundo digital, el robo de tarjetas de crédito y el abuso de códigos telefónicos.

Más bien fue el mayor acoso a los B.B.S. de la historia mundial. El 7, 8 y 9 de marzo de 1990 se incautaron alrededor de 42 sistemas informáticos.

Téngase en cuenta que en EE.UU. hay aproximadamente 30,000 BBS y existen mas de 1 de cada cinco con malas intenciones respecto a códigos y tarjetas.

Los Estados que fueron objeto de esta operación fueron Cincinatti, Detroit, Los Ángeles, Miami, New York, Phoenix, Tucson, Richmond, San Diego, San José, San Francisco y Pittsburg. Chicago por su parte tuvo su propia confiscación con sus servicios secretos.

En estos Estados actuaron 150 miembros del servicio secreto que asesoran y actuación con Brigadas de la Policía Estatal y local y expertos en seguridad de telecomunicaciones, la Policía de Delitos informáticas entre otras fuerzas.

Esto sucedió hace 10 años ¿Cómo será hoy? Por eso la Policía Cibernética y el servicio secreto del futuro tendrán que trabajar imponiendo la ley con su cabeza y no con pistolas ni patrullaje, puesto que cada día avanza mas la revolución de ordenadores, modos de operar muy sofisticado, moderno, y difícil de detectar y probar por la utilización de medios y métodos de alta tecnología.

Para que se tenga una mera idea del severo golpe a toda la cancha ciberespacial y al crimen organizado del bajo mundo digital la operación “Diablo del Sol” logró:

- Incautación de 23,000 disquetes conteniendo datos ilegítimos juegos pirateados, códigos robados, el texto y software completo dichos disquetes ofrecen una fuente gigantesca y embarazosamente rica de posibles procedimientos criminales. También una cantidad hasta ahora desconocida de juegos y programas legítimos, correos supuestamente privados de los B.B.S., archivos comerciales y correspondencia personal de todo tipo.
- Se apagaron por completo los 30,000 BBS por todos los EE.UU. y fueron enviados al laboratorio de Investigación Informáticas del Servicio Secreto junto con los disquetes y el material impreso, evidencia esta que hoy esta en manos de la Policía.

Algunas recomendaciones finales

Al recibir un "alerta de virus" por medio de un correo electrónico verifique la información directamente con su proveedor de Antivirus.

No reenvié la información; evite las cadenas.

La Universidad de Oregon resume de la siguiente manera las principales características de los engaños por INTERNET:

- Una advertencia sobre un nuevo virus que deberías enviar a todos tus conocidos.
- Una advertencia sobre un fraude electrónico que deberías enviar a todos tus conocidos.
- Un pedido de ayuda para los necesitados o alguna otra causa que te solicita que a su vez la distribuyas a todos tus conocidos.
- Una oferta de dinero que podrías ganar por cada nuevo destinatario a quien le envíes esa oferta.
- Una aseveración de que por cada mail que le envíes a un nuevo destinatario, un tercero con quien simpatizas recibirá algún beneficio.

Antes de realizar cualquier reenvío verifique lo siguiente:

- La fecha *original* en que el mensaje fue creado y enviado, y la fecha de expiración del mensaje, si la hay;
- El remitente original;

- La existencia y veracidad de dichos de personas u organizaciones, por medio de sus páginas Web (URL's genuinos);
- Si el mail se refiere a alguna causa o evento, la existencia, fecha y documentación citada;
- En caso de que hayas decidido reenviar el correo, protege la privacidad de los destinatarios.

http://www.revistainterforum.com/espanol/articulos/Tecnologica_040101.html

"Crimen Electrónico: El delito del siglo XXI"

Resultados y comentarios de la tertulia **INTER-FORUM & CCE** celebrada Junio 4 del 2001 en el Centro Cultural de España

Con el Lic. Valentín Arteaga y el Lic. Genaro D. Salom

El Centro Cultural de España e **INTER-FORUM**, revista electrónica celebraron el pasado lunes 4 de Junio la tercera Tertulia **INTER-FORUM,** en esta ocasión con el Lic. Valentín Arteaga quien converso sobre el tema "Crimen Electrónico: El delito del siglo XXI".

El Lic. Arteaga se refirió a la frecuente confusión por parte del publico cuando escucha la expresión Crimen Electrónico. Agregó que muchas veces se utilizaba indistintamente el termino Crimen Electrónico para señalar crímenes o delitos cometidos utilizando como medio artefactos electrónicos de alta tecnología. Arteaga señaló como delito electrónico el espionaje y / o interferencia de las comunicaciones, los fraudes con tarjetas de crédito, entre otros. También señaló que en muchos lugares se daba lo que se ha denominado como "Robo de identidad" situación en la que el delincuente, haciéndose pasar por la víctima, utiliza las nuevas tecnologías para realizar transacciones financieras.

Valentín Arteaga es Consultor de Negocios en el área de seguridad. Como Criminalista cubano ha dedicado muchos años a la cátedra universitaria, tanto en Cuba como en la República Dominicana. Cuenta con más de 25 años de experiencias en investigación criminal, desde la escena del crimen hasta el juicio oral. Ha participado en procesos de investigación de casos internacionales, tanto para organismos internacionales como para otras instancias. Las temáticas de su especialidad incluyen Criminalística, Criminología y Derecho Penal.

Genaro Salom, Director de Operaciones de **INTER-FORUM,** se refirió a las problemáticas relacionadas con la conectividad y a las medidas preventivas para evitarlas. "La mayor parte de los problemas que enfrentan los usuarios, tanto a nivel

de computadoras personales o de los equipos en las empresas, se relaciona con el área de seguridad en los sistemas" dijo Salom. Agrego que esta problemática se concentra en tres aspectos "Primero la ausencia de sistemas de antivirus actualizados; segundo la ausencia de firewall o de sistemas de seguridad alternos; y tercero la falta de actualización de los Browsers como Internet Explorer 5.5". Indicó que "tomar estas medidas preventivas contribuyen a reducir en un 90% aproximadamente riesgos en las áreas de seguridad de los equipos. La constante actualización de estos sistemas es imprescindible para el eficiente y seguro funcionamiento de los equipos".

En lo referente a la primera problemática, la de los virus, señalo que la situación de proveedores internacionales, como es el caso de MSN y Hotmail.com que ofrecen a sus usuarios altos niveles de seguridad y depuración de virus. En comparación con los servidores locales, que ofrecen muy poca o ninguna protección a sus clientes, el Lic. Salom señalo que desconoce si las empresas locales tienen o no instalado en sus servidores sistemas antivirus, pero que es realmente sencillo hacerlo, ya que esto es solo un software. Al ofrecer este servicio estarían ofreciendo un servicio mas completo a los usuarios que no saben como protegerse. Agrego que en el caso de Hotmail.com estos ofrecen un sistema de depuración automática a sus usuarios con McAffe VirusScan.

En cuanto a las regulaciones internacionales de Internet de lo que se puede y no se puede, estas deben ser establecidas por un organismo internacional que dicte los parámetros regulatorios a aplicar. Este organismo debe contar con autonomía, autoridad y jurisdicción internacional.

En lo referente al SPAM, el Lic. Salom señaló que con la integración del INTERNET a las telecomunicaciones, y bajo el concepto de la libre expresión y tomando en consideración el comercio electrónico de negocio a negocio (B2B, Business to business) y negocio a cliente (B2C Business to Client) no debería existir ninguna regulación prohibitiva, como no existe en ningún lugar del mundo ninguna regulación para los correos físicos. Sin embargo, agregó, pudiesen existir regulaciones referentes a las características de esos envíos, debido al rápido desarrollo del Internet. Una de ellas pudiese ser el limitar el peso en Kb. y tamaño de estos correos enviados por la entidad comercial o privada.

Al evento asistieron abogados, estudiantes de temino de ciencias jurídicas, personas de seguridad electrónica y banca. La dinámica de la actividad permitió a los presentes una activa participación, compartiendo sus interrogantes e información sobre casos que habían conocido indirectamente por los medios de comunicación.

Una de las interrogantes de los presentes fue en lo referente a las regulaciones del crimen electrónico, a lo que Arteaga respondió que aun los países mas avanzados en materia penal no habían establecido aun condenas especificas como tal hacia el denominado crimen electrónico. Que más bien los delincuentes eran juzgados tipificando su crimen en base a las legislaciones vigentes de cada país, y tipificando el delito cometido como fraude, falsificación u otro. Sin embargo, entiende que ya están revisándose las legislaciones y pronto empezaran a realizarse cambios en este sentido. En algunos países como Estados Unidos, España e Inglaterra, entre otros, están legislando y creando nuevas leyes que protejan de este tipo de manifestación delictiva.

INTER-FORUM, tiene por objetivo promover la educación y la cultura a través de sus programas y servicios. Para mayor información sobre esta y otras tertulias pueden enviar correo a info@revistainterforum.com. La próxima tertulia se realizará con la Lic. Gisela Vargas, con el tema "El libro electrónico: una nueva oportunidad para autores, editores y lectores".

http://www.revistainterforum.com/espanol/articulos/061001delitoelec.html