



# SEGURIDAD EN COMERCIO ELECTRÓNICO

*Seguridad de la Información:  
“Un enfoque orientado a la defensa proactiva  
y al análisis y planteo de soluciones”*

**Autor: Matías D. Adés**



**SEGURIDAD EN COMERCIO ELECTÓNICO***Seguridad de la Información:**“Un enfoque orientado a la defensa proactiva y al análisis y planteo de soluciones”***Resumen**

El Comercio Electrónico es cualquier acción de compraventa de productos, servicios e información a través de medios electrónicos, es decir a través de redes informáticas como Internet. Si bien cuando se acopla la Internet con el comercio los resultados son positivos puesto que la competencia es más "global" y los precios disminuyen, también se deben tener ciertas precauciones ya que no dejamos de estar expuestos a los riesgos que implica el uso de este novedoso y fácil, pero a la vez gigantesco y lleno de inseguridades, "mundo virtual". Por este motivo, propongo introducir al lector a lo que es Comercio Electrónico brindando ciertos conceptos clave para que logre entender de qué se trata, dando también algunas recomendaciones desde el punto de vista de la seguridad al momento de navegar por Internet con el objetivo de comprar. A su vez, pretendo ampliar el material con un enfoque orientado al análisis e investigación proponiendo soluciones basadas en software a los posibles problemas ocasionados por la presencia de Malware que, evidentemente, amenaza la realización de transacciones comerciales electrónicas seguras.

**Abstract**

The Electronic Commerce (e-Commerce) is the buying and selling of products, services and information through electronical means, such as the Internet. Although when the Internet with the commerce is reconciled the results are positive since the competition is much more "global" and prices fall. We also have to consider certain precautions as we aren't free to be exposed to the risks that implies the use of this novel and easy, but at the same time gigantic and full of insecurities, "virtual world". For that reason, I mean to introduce you to the e-commerce offering some key concepts to make sure the understanding of what we are going to deal with. This will include certain recommendations from the point of view of the security at the moment of browsing over the Internet with the goal of buying. Meanwhile, I pretend to expand the material with an approach aimed at the analysis and research, suggesting software-based solutions to the possible problems caused by the presence of Malicious Software (Malware) that, evidently, threatens the accomplishment of safe electronic commercial transactions.

**Autor / Author:** Matías D. Adés – arcticeye@gmail.com

**Palabras Clave:** seguridad en comercio electrónico, e-commerce, seguridad informática, seguridad de la información, malware, software malicioso.

**KeyWords:** electronic commerce security, information security, malware, malicious software, informatic security.

**Fecha / Date:** Agosto de 2007 / August 2007

## Índice de contenido

<b>Introducción.....</b>	<b>4</b>
<b>Lo que hay que saber: Seguridad en Componentes de Redes.....</b>	<b>5</b>
<b>Bases para realizar transacciones en el Comercio Electrónico.....</b>	<b>5</b>
Negocio a Cliente (B2C - Business to Consumer).....	7
Negocio a Negocio (B2B - Business to Business).....	7
Cliente a Cliente (C2C - Consumer to Consumer).....	7
<b>Seguridad Electrónica.....</b>	<b>8</b>
Seguridad en relación al portal.....	8
Seguridad en relación al vendedor.....	9
Seguridad en relación al canal de comunicación.....	10
Seguridad en relación al cliente.....	13
<b>Malware y Comercio Electrónico.....</b>	<b>14</b>
Cookies.....	15
¿Qué son y para qué se usan?.....	15
Problemas que pueden ocasionar a los usuarios de Comercio Electrónico.....	15
Análisis de los Interrogantes.....	15
Respuesta a las Problemáticas.....	17
Soluciones Existentes.....	17
Soluciones Software Propuestas.....	17
Keyloggers.....	18
¿Qué son y para qué sirven?.....	18
Tipos de keyloggers.....	18
Problemas que pueden ocasionar a los usuarios de Comercio Electrónico.....	18
Soluciones Existentes.....	19
Soluciones Software Propuestas.....	20
Pharming.....	20
¿Qué es?.....	20
Tipos de ataque pharming.....	20
Principales usos y problemas que ocasiona en Comercio Electrónico.....	21
Soluciones Existentes.....	21
Soluciones Software Propuestas.....	22
Phishing.....	22
¿Qué es y con qué fin se utiliza?.....	22
Principales usos y problemas que ocasiona en Comercio Electrónico.....	22
Soluciones Existentes.....	23
Soluciones Software Propuestas.....	24
Spyware.....	25
¿Qué es y para qué se usa?.....	25
Composición.....	25
Problemas que ocasiona a los usuarios de Comercio Electrónico.....	25
Soluciones Existentes.....	26
Soluciones Software Propuestas.....	26
<b>Resumiendo: Guía rápida para comprar en Internet - Ejemplo.....</b>	<b>27</b>
<b>Conclusión.....</b>	<b>30</b>
<b>Fuentes.....</b>	<b>31</b>

## Introducción

El comercio en occidente se remonta varios siglos antes del nacimiento de Cristo en lo que se llamó *la media luna fértil*. Ríos como el Tigris y el Eufrates permitieron que los hombres que allí se habían establecido crearan sistemas económicos propicios para el intercambio.<sup>1</sup> A lo largo de toda la historia se evidenció un gran crecimiento en el desarrollo y producción de medios de comunicación y de transporte que permitieron conectar ciudades y continentes ubicados en los extremos del planeta dando sustento al sistema de comercio. Hoy, en la *era de la información*, somos testigos de esta realidad. Las diversas redes de comunicación que se extienden alrededor del mundo que están al alcance de gran parte de la población mundial, y a su vez la facilidad de transporte aéreo, marítimo y terrestre, dan sustento para justificar la aparición del Comercio Electrónico. La Internet, una de las actuales y más extendidas redes mundiales de información, no conoce las fronteras, y en el ámbito del comercio posee el potencial de ofrecer oportunidades únicas y decisivas a organizaciones de cualquier tamaño: es rápido, razonablemente confiable y barato.

El fraude en el comercio tradicional es un tema que preocupa desde la antigüedad, y la aparición del Comercio Electrónico obliga claramente a replantearse si los medios sobre los que se basa son susceptibles a este crimen. Las experiencias acontecidas desde que se hace uso de esta nueva forma de comercio lo demuestra: A la hora de comprar y vender por Internet, nos encontramos en un mundo virtual donde las reglas cambian, surgiendo nuevos problemas e incluso agudizando algunos de los ya existentes. Para operar en este nuevo ambiente debemos estar preparados, conociendo la naturaleza que lo rige y disponiendo de las herramientas y soluciones que nos permitan, en lo posible, tomar acciones de defensa proactivas.

Debido a la problemática planteada, este trabajo tiene como objetivos brindar un panorama general para comprender de qué se trata el Comercio Electrónico, abordando el tema de la seguridad desde tres perspectivas diferentes: el prestador del servicio, el canal de comunicación y el cliente. A su vez, y del lado del cliente, si bien se pretende ampliar el material con un enfoque orientado al análisis e investigación sobre Malware que afecta al Comercio Electrónico planteando soluciones basadas en software, también se dan a conocer muchas de las opciones de defensa ya existentes.

---

1 <http://www.slideshare.net/ROBINHOOD/la-historia-del-comercio-y-los-negocios/>

## Lo Que Hay Que Saber: Seguridad En Componentes De Redes

Al hablar de redes se debe considerar la existencia de computadoras, medios de comunicación, e información que viaja, de computadora a computadora, por esos medios.

Los aspectos de seguridad que se deben considerar en las redes son [Graziosi, 2007]:

- ✓ **Confidencialidad:** La información que se transmite puede ser vista por personas que no deberían tener acceso a ella mientras está siendo transmitida.
- ✓ **Autenticidad:** La información que se transmite puede ser capturada mientras está siendo transmitida, **alterada la identidad del origen** y posteriormente retransmitida al destino original.
- ✓ **Integridad:** La información que se transmite puede ser capturada mientras está siendo transmitida, modificada y posteriormente retransmitida al destino original.
- ✓ **Disponibilidad:** No se puede transmitir información por falta o falla de alguno de los elementos que intervienen en la comunicación.
- ✓ **Repudio:** La información enviada por un emisor es negada en la recepción por el destinatario de la misma o bien la información recibida por un receptor es negada de haber sido enviada por el emisor.

Si bien lo fundamental es la disponibilidad, ya que si no existe no puede pensarse en el resto de los aspectos, al hablar de Seguridad en el Comercio Electrónico, aquellos que más inciden son la confidencialidad, la autenticidad, la integridad y el repudio.

Así, es importante considerar estos conceptos al hablar de Comercio Electrónico, puesto que parte importante de la transacción comercial se realiza por medio de Internet, la “red de redes”.

## Bases Para Realizar Transacciones En El Comercio Electrónico

El Comercio Electrónico es muy utilizado. Para tener una idea, tal es el caso, que en Europa marca máximos históricos en 2006, alcanzándose los 637 millones de euros en el segundo semestre de 2006 y superando los dos mil millones de euros durante todo el año pasado.<sup>2</sup> La siguiente tabla demuestra también el incremento notable producido por este sector en América Latina.<sup>3</sup>

2 Según informe de la Comisión del Mercado de las Telecomunicaciones con fecha 13/02/2007.  
<http://www.cmt.es>

3 Publicada por la Cámara Argentina de Comercio Electrónico (2006). <http://www.cace.org.ar>

Datos Estadísticos de América Latina	1999	2000	2001	2002	2003	2004	2005
Usuarios de Internet (mi)	10,2	16,2	22,6	32	44	58,36	-
Usuarios Internet domésticos activos (mi)	5,3	8,5	10,5	14,5	19,8	25,72	-
PCs (mi) (base instalada)	21,3	26	31	38,5	42,4	48,7	54,02
Celulares (mi)	36,9	54,2	67,6	75,8	93	102	115
E-Commerce (US\$bi)							
- B2B (US\$bi)	0,4	0,9	2,9	6,5	12,5	21,5	33,1
- B2C (US\$bi)	0,2	0,5	1,3	2,3	4,5	7,8	12
Gastos de Publicidad Online (US\$ bi)	NS	53,8	87,7	79,2	100,6	105,7	111,9
% gastos de publicidad total	0,20%	0,50%	1,00%	1,80%	2,20%	2,20%	2,20%
Gastos en IT (US\$bi)	27,2	28,7	30,0	30,3	32,2	33,8	35,1

Esto es para remarcar que más son los usuarios internautas que usan este medio de compra año a año, por lo cual es necesario hacer ojo en los aspectos de la seguridad.

Una definición interesante de Comercio Electrónico es la siguiente:

El Comercio electrónico es una manera de hacer negocios, vendiendo o comprando productos, información y servicios por Internet, bajo ciertos estándares de seguridad.<sup>4</sup>

Esta definición hace mención a la compraventa usando Internet, lo cual no implica la no existencia de otros medios electrónicos para su realización; la realidad es que la mayoría de las operaciones en Comercio Electrónico son realizadas a través de Internet por su amplia envergadura. Por otro lado, también se mencionan los *estándares de seguridad*, que son una de las medidas de seguridad a destacar en este trabajo.

Ahora que se tiene una idea sencilla de lo que es el Comercio Electrónico (e-commerce) y de su importancia, se presentarán las formas que existen de hacer negocios a través de Internet. Esta clasificación resulta interesante tenerla presente, puesto que existen diferentes sitios en la red dedicados a una u otra de dichas formas de negociar. Por esta razón es importante saber distinguirlas según el rol que se cumpla en la compra-venta y con quién se quiera realizar dicha transacción.

4 Extraído de: <http://www.panamacom.com/seguridad.html>

**Negocio A Cliente (B2C - Business To Consumer)**

Es un tipo de venta electrónica mediante la cual la empresa ofrece sus productos y/o servicios por Internet a sus clientes. Es una tienda virtual en la que el cliente puede ver los productos de la empresa teniendo la opción de compra. Esta modalidad de "abrir" los negocios al público a través de Internet en general obedece a definiciones estratégicas globales que se trazan las empresas cuyos objetivos entre otros serán: disminución de costos, segmentación del mercado, creación de una vidriera global, aceleración de los mecanismos de distribución y aumento del grado de satisfacción del cliente.<sup>5</sup>

**Negocio A Negocio (B2B - Business To Business)**

Es una rama del Comercio Electrónico referida a las transacciones realizadas en el ámbito de distribuidores y proveedores. Usualmente este tipo de comercio es más restringido que los demás, e involucra a los suplidores y distribuidores de productos. Esta rama es muy amplia y se puede desarrollar de diversas formas, desde programas propietarios en donde el suplidor/distribuidor debe comprar el mismo software para transaccionar, hasta el uso de la Internet como plataforma múltiple y neutral. Los factores primordiales que impulsan a las industrias a crear una estrategia de Comercio Electrónico de negocio a negocio son básicamente la reducción de gastos y el aumento de eficiencia. Además, entre sus usos, el proveedor puede mostrar su inventario a los distribuidores, con diferentes precios dependiendo de los clientes, y todo protegido con claves que permiten la revisión de estados de cuenta y los pagos de las mismas.<sup>6</sup>

**Cliente A Cliente (C2C - Consumer To Consumer)**

Modalidad de Comercio Electrónico en la cual las operaciones comerciales se realizan entre clientes, como los sitios en donde se realizan subastas (ej. DeRemate.com).<sup>7</sup> Aquí un cliente puede hacer el papel de vendedor subastando un solo artículo; en otras palabras, cualquier particular puede colocar a la venta un producto en un sitio especial al efecto, el cual brinda una plataforma para todos los ciudadanos que deseen vender directamente sus bienes o artículos. Estos sitios no necesariamente deben ser comerciales; durante el 2000 uno de los sucesos de mayor impacto en Internet fue el sitio creado por universitarios norteamericanos para el intercambio gratuito de música. En menos de un año obtuvo decenas de millones de asociados, y recibió una demanda de las casas discográficas, pero creó un concepto de sistema de distribución descentralizado aplicable con fines comerciales.<sup>8</sup>

Antes de entrar en la sección precedente se quiere dejar en claro que, como parte de este documento va dirigido a usuarios que desean hacer compras a través de la Web, se va a centrar en seguridad B2C y C2C.

5 <http://comercio-electronico.sextageneracion.com/>

6 <http://todocomercioelectronico.blogspot.com/2007/06/categorias-business-to-business-y.html>

7 <http://www.glosariointernet.com/68/c2c.htm>

8 Extraído de: [http://www.wikilearning.com/curso\\_gratis/globalizacion\\_y\\_gestion\\_on\\_line-categorias\\_de\\_comercio\\_electronico\\_b2b\\_b2c\\_c2b\\_c2c\\_etc/13653-9](http://www.wikilearning.com/curso_gratis/globalizacion_y_gestion_on_line-categorias_de_comercio_electronico_b2b_b2c_c2b_c2c_etc/13653-9)

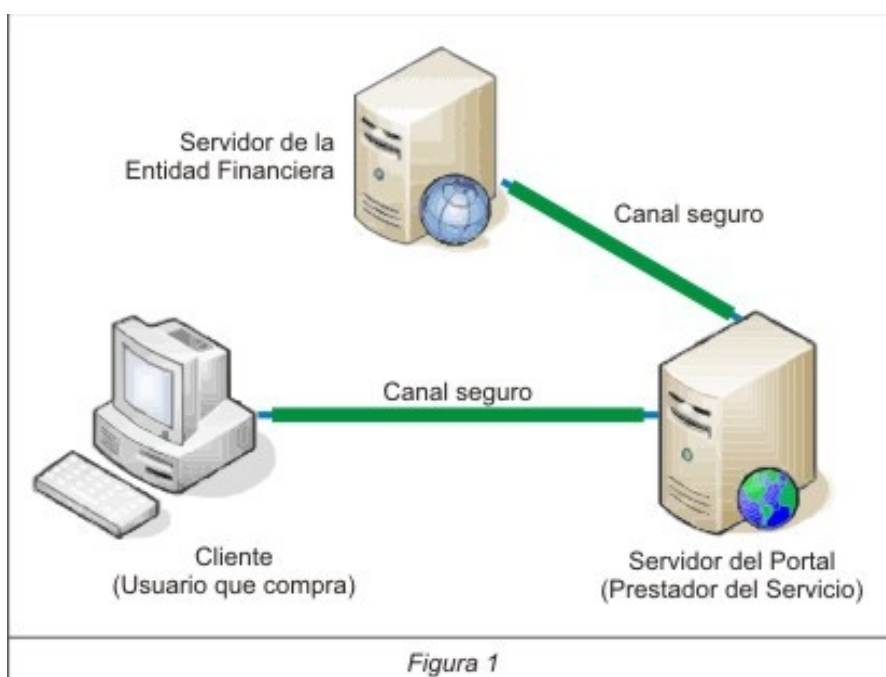


## Seguridad Electrónica

Muchas personas perciben que comprar por Internet es inseguro, pero en realidad es lo suficientemente seguro si se toman las medidas adecuadas de seguridad. Muchos de los casos de fraude en Internet se deben a que los números de las tarjetas son robados fuera de Internet. Ya que el proceso de comprar en línea no exige firmas (todavía), es relativamente fácil hacer compras con tarjetas robadas, pero no tanto robar los números en la Internet.<sup>9</sup> De cualquier manera, las entidades bancarias están tomando medidas de seguridad en lo que respecta a los hábitos de compra de los consumidores que poseen tarjetas de crédito. Así, por ejemplo, si un individuo obtiene el número de tarjeta, junto con otros datos necesarios de la víctima, y utiliza toda esta información para comprar por Internet por un monto X, el banco puede determinar la existencia de fraude analizando y comparando los flujos normales de dinero de su cliente; al encontrarse valores aberrantes, se procedería al congelamiento de la tarjeta y a una posterior investigación.

Pero atención, se quiere dejar en claro que *nada* es completamente seguro, ninguno de los métodos que se presentan aquí ni ninguno en su existencia; más bien se mejora la seguridad o se disminuye, pero no se evita nunca en un 100%.

Bien sabemos, o al menos nos damos una idea, que toda transacción comercial está compuesta por cuatro partes: el portal, el vendedor, la comunicación y el cliente, (figura 1) y no es una excepción para el caso del Comercio Electrónico. Propongo esta clasificación para abordar a continuación el tema de la seguridad.



### Seguridad En Relación Al Portal

En un portal B2C o B2B es muy probable que el mismo prestador del servicio sea el dueño del portal, y será quien a su vez proporcione la seguridad del mismo. Es decir, la seguridad de un sitio Web es responsabilidad del proveedor del hospedaje (hosting) y los encargados de diseñar y mantener el sitio, así que es importante que

<sup>9</sup> Extraído de: <http://www.panamacom.com/seguridad.html>



se mantenga actualizado y tenga conocimiento y experiencia en el tema.

Bien se debe saber que un sitio Web NO debe enviar los números de tarjeta de crédito por e-mail, ni debe guardarlos en alguna base de datos para uso posterior. La manera correcta es enviando esta información por **canales seguros** a la institución financiera que procesa las tarjetas. Si el cliente vuelve a comprar en la tienda virtual, probablemente no tenga que escribir su información nuevamente, pero sí tendrá que escribir el número de tarjeta cada vez.<sup>10</sup> Esto está más relacionado al tema *seguridad con respecto al canal de comunicación*, que se presentará posteriormente con mayor detalle.

Nunca sabemos si el portal es lo suficientemente seguro, no sabemos qué recaudos se tienen en cuenta por parte del hosting...qué políticas, etc. Por ello, lo más recomendable es comprar en sitios reconocidos y seguros, con **certificados de seguridad**. ¿Cómo nos damos cuenta qué sitio es reconocido o no?<sup>11</sup>

- Por la publicidad que se haga en los distintos medios, no solo en Internet, sino la radio, el periódico o la televisión; además, por la experiencia que otros amigos hayan tenido;
- estando al tanto de las noticias acerca del Comercio Electrónico podemos tener una idea de la seguridad en los sitios de venta online;
- en caso de ser un sitio nuevo, buscando si tiene identidad, denominación legal y datos de ubicación física tales como su dirección, teléfono y fax. También es importante el nombre o marca de comercialización de la empresa y sus productos;
- si se cuenta con políticas de privacidad, sobre todo cuando la transacción implica que se den a conocer algunos datos de carácter privado como números de tu tarjeta de crédito;

Algunos sitios reconocidos donde se puede comprar en Argentina son: mercadolibre.com.ar (C2C), deremate.com (C2C), masoportunidades.com.ar (C2C); internacionales: ebay.com (C2C), amazon.com (B2C). Por supuesto existen muchos más, pero es tarea del lector investigar siguiendo las pautas que se han dejado.

### Seguridad En Relación Al Vendedor

Aquí se darán las pautas generales sobre qué tener en cuenta para elegir un vendedor confiable para el caso de la modalidad de comercio C2C. En la modalidad B2C, desde el momento que se ingresa a la página se tendrá una imagen anterior del vendedor si es que ya se lo conoce (ej. Dell, IBM, etc.); si no fuese así, quizás se necesite investigar más acerca de él. Cabe aclarar que es bastante difícil distinguir entre la seguridad en relación al vendedor y al portal cuando se trata de B2C.

Muchos son los usuarios que no saben utilizar las ventajas que brindan los sitios de Comercio Electrónico y salen defraudados por vendedores dedicados a encontrar la forma de estafar a aquellos que no pueden distinguir entre un buen vendedor y un defraudador. Existen ciertas variables que nos permiten identificar y nos alertan, en mayor o menor medida, acerca de la calidad de prestador de servicio que tiene un vendedor.

<sup>10</sup> Extraído de: <http://www.panamacom.com/seguridad.html>

<sup>11</sup> Más información en: <http://www.liderempresarial.com/num103/9.php> y [http://www.profeco.gob.mx/ecomercio/ecomercio\\_ejerce.asp](http://www.profeco.gob.mx/ecomercio/ecomercio_ejerce.asp)

Al buscar un producto lo primero que el comprador tiene que saber es si es nuevo o usado; puede que se busque un producto nuevo, se comparen precios de dos o más vendedores y haya grandes diferencias (o en el peor de los casos no), y resulte ser que uno de ellos vendía el mismo producto pero usado; si bien quizás no concierna a este aspecto de seguridad informática, decidí que es oportuno hacerlo saber en este momento.

- Todo vendedor, en la mayoría de los sitios de compra-venta por Internet, tiene una *calificación*, que es el resultado de la diferencia entre las calificaciones positivas y negativas de los usuarios. En algunos sitios se toman "calificaciones de usuarios únicos", o sea la primera calificación que se reciba de un usuario; si éste lo califica por otras operaciones, éstas ya no sumarán ni restarán en el puntaje general. Como primer medida es importante tener en cuenta esto de las calificaciones ya que son los mismos clientes de un vendedor que lo están evaluando; en general, sería bueno tener en cuenta prestadores con calificación positiva de por arriba del 95%.
- Otro aspecto que hay que analizar en conjunto con el anterior, es *cuándo se recibieron las calificaciones*; puede que un proveedor tenga un 10% de calificaciones negativas pero sólo en sus comienzos (ej. hace 2 años) y que luego todas las demás hayan sido positivas; en este caso, personalmente, este proveedor sería más confiable que otro con el mismo porcentaje pero que haya recibido recientemente parte de las calificaciones negativas.
- Un tercer factor son las *ventas que realizó* el prestador, lo que nos demuestra la actividad del mismo; también, si el sitio nos lo permite, es probable que pueda conocerse la cantidad de artículos vendidos en los últimos días como en los últimos meses, o en años.
- Tómese un tiempo, si el portal lo permite, vea los *comentarios* positivos y los negativos que dejan los usuarios a los vendedores, eso le dará un panorama de cómo éste realiza sus operaciones, su eficiencia como vendedor y de la disponibilidad de los productos que vende, entre otras cosas.

### Seguridad En Relación Al Canal De Comunicación

Los canales de comunicación rara vez se consideran seguros. Sea en transacciones B2B, C2C o B2C, debido a que en la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos.<sup>12</sup> Por ello, una de las cuestiones a considerar a la hora de comprar por Internet es la que se plantea como interrogante a continuación: ¿Cómo nos aseguramos de que la información confidencial que enviamos a un proveedor (o vendedor) vía Web tenga poca oportunidad de *ser entendida* por alguien que acceda a la misma en forma ilegítima?, en otras palabras: ¿Queremos que nuestras confidencias (nuestros números de tarjeta de crédito, nuestros saldos en bancos, etc) sean vistos por personas desconocidas?<sup>13</sup>

El hecho de que la información que fluye por la Internet pueda ser "intervenida" por terceras personas se mitiga usando **encriptación de datos**. Los métodos de encriptación de datos hoy en día utilizados son bastante seguros y eficientes para

12 Extraído de: [http://html.rincondelvago.com/seguridad-de-la-informacion\\_criptografia.html](http://html.rincondelvago.com/seguridad-de-la-informacion_criptografia.html)

13 Más información en: <http://www.seguridadenlared.org/es/index25esp.html>

proteger la confidencialidad, aunque nunca lo suficiente. Esto cambiará cuando existan computadoras personales lo suficientemente rápidas para descifrar un código en minutos. Todavía faltan algunos años, y para ese entonces se usarán mejores y distintos métodos de encriptación de datos.<sup>14</sup>

La **criptografía**, es un conjunto de procedimientos para cifrar mensajes de forma tal que, si son interceptados, no se pueda entender su contenido. Cuando se compra por Internet se hace uso de un navegador Web, y en cada transacción por este medio se interviene un protocolo llamado HTTP (Hypertext Transfer Protocol). HTTP no asegura ni la confidencialidad, integridad o autenticidad, pero sí lo hace en cierto modo HTTPS. El protocolo *HTTPS* (S: Secured) es una versión segura de HTTP que implementa un canal de comunicación seguro y basado en SSL (Secure Socket Layer) entre el navegador del cliente y el servidor HTTP.<sup>15</sup> SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía<sup>16</sup>, y es necesario que tanto el cliente como el portal lo tengan instalado en sus respectivos sistemas para que funcione.

A diferencia de HTTP, HTTPS, antes de enviar los datos realiza algunas acciones previas. En una de ellas, el servidor HTTPS envía un certificado al cliente.

Un **certificado de clave pública** es un documento que certifica que el interlocutor (el servidor HTTPS) es quien realmente dice ser; esto se hace para evitar que un atacante pueda hacerse pasar por el servidor y recibir la comunicación segura en su lugar.<sup>17</sup>

Más arriba se mencionó que HTTPS implementa SSL, lo cual no es la única solución y presenta los siguientes inconvenientes<sup>18</sup>:

- Sólo protege transacciones entre dos puntos (el servidor web comercial y el navegador del comprador). Sin embargo, una operación de pago con tarjeta de crédito involucra como mínimo tres partes: el consumidor, el comerciante y el emisor de tarjetas.
- No protege al comprador del riesgo de que un comerciante deshonesto utilice ilícitamente su tarjeta.
- Los comerciantes corren el riesgo de que el número de tarjeta de un cliente sea fraudulento o que ésta no haya sido aprobada.

Claramente se ve que este protocolo no es del todo seguro y que se hace necesaria la invención de uno específico para el pago. Por tal motivo, en el año 1995 se creó *SET* (Secure Electronic Transaction). Pero quienes estén al tanto de esto se preguntarán: ¿Por qué SET no goza de la popularidad de SSL, si se supone mejor adaptado?<sup>19</sup>:

En primer lugar, su despliegue está siendo muy lento. Exige software especial, tanto para el comprador (aplicación de monedero electrónico) como para el comerciante (aplicación POST o terminal de punto de venta), que se está desarrollando con

14 Extraído y adaptado de: <http://www.panamacom.com/seguridad.html>

15 Extraído y adaptado de: <http://www.programacionweb.net/articulos/articulo/?num=411>

16 Extraído de: [http://es.wikipedia.org/wiki/Transport\\_Layer\\_Security](http://es.wikipedia.org/wiki/Transport_Layer_Security)

17 Extraído de: <http://www.programacionweb.net/articulos/articulo/?num=411>

18 Extraído de: <http://www.iec.csic.es/criptonomicon/susurros/susurros08.html>

19 Extraído de: <http://www.iec.csic.es/criptonomicon/susurros/susurros08.html>

lentitud. En segundo lugar, aunque varios productos cumplan con el estándar SET, esto no significa necesariamente que sean compatibles. Este es un problema que exige mayores esfuerzos de coordinación y más pruebas a escala mundial para asegurar la interoperabilidad. Sus puntos fuertes son también su talón de Aquiles: la autenticación de todas las partes exige rígidas jerarquías de certificación, ya que tanto los clientes como comerciantes deben adquirir certificados distintos para cada tipo de tarjeta de crédito, trámites que resultan engorrosos, cuando no esotéricos, para la mayoría de los usuarios.

En definitiva, SET es un elefante de gran tamaño y fuerza, pero de movimientos extraordinariamente pesados. SSL es una liebre que le ha tomado la delantera hace años. No es tan perfecto, no ofrece su seguridad ni sus garantías, pero funciona. Y lo que es más: ¡el usuario de a pie no tiene que hacer nada!

Los siguientes son consejos. Ciertos pueden estar referidos quizás a la seguridad en relación al cliente, pero se considera oportuno mencionarlos aquí por la relación que tienen con el tema desarrollado en esta sección<sup>20</sup>:

- Nunca, absolutamente nunca, enviar datos financieros en un mensaje de correo electrónico ordinario.
- Para llevar a cabo compras a través de Internet, utilizar únicamente portales seguros.

De esta regla se desprende una consecuencia lógica: no teclee nunca sus datos financieros en un formulario de un servidor Web que no sea seguro. De hacerlo, sus datos viajarían sin cifrar, expuestos en cada nodo del camino, tal y como ocurre con el correo electrónico ordinario. Por esta razón, su navegador le avisa antes de enviar los datos en un formulario no seguro. Se hace pues imprescindible diferenciar cuándo uno se encuentra en un servidor seguro y cuándo no. De esto se encargan los actuales navegadores Web, es decir, de alertar al usuario a través de diversos signos como ser:

1. La configuración por defecto de los navegadores permite avisar mediante un mensaje al usuario, cuando se está por ingresar en un servidor seguro solicitando nuestra conformidad.
2. Una vez accedido el sitio seguro, se verá que la URL comienza por https en lugar de http. Compruébese siempre.
3. El pequeño icono de la llave (o candado) que aparece en la esquina inferior izquierda de la pantalla se transforma: la llave se vuelve completa o el candado se cierra, y su fondo se resalta.

Esto lleva al tercer consejo...

- Comprobar siempre las características de seguridad de un sitio antes de comprar en él.
- Mantener actualizado el navegador y/o los certificados incorporados en él.

---

<sup>20</sup> Extraído y adaptado de: <http://arte.mundivia.es/astruc/doctxt10.htm>

## Seguridad en relación al cliente

En este ámbito conviene tener presente las siguientes recomendaciones [Coudert y otros, 2007]:

- Navegar en portales conocidos o extremar las precauciones antes de comprar en un sitio mínimamente dudoso o poco conocido.

Por ejemplo, existen ciertos portales C2C como DeRemate.com, mercadolibre.com, ebay.com, o B2C como Dell, Yahoo, Amazon, ebay que son muy conocidos y donde compra mucha gente. Se aconseja al lector que si no sabe si un sitio es dudoso o no, o si no tiene idea de dónde comprar, antes de hacerlo, consulte a amigos que lo hayan hecho y que les haya dado buen resultado, o pregunte a gente con experiencia que ya haya hecho transacciones por este medio.

- En los sistemas de autenticación de usuario basado en contraseñas no utilizar las mismas contraseñas en los sistemas de alta seguridad y en los de baja seguridad.

Puede ocurrir que alguien que conoce la contraseña de una persona, por haber accedido a un sitio de baja seguridad, pueda averiguar dónde accede dicha persona para hacer transacciones seguras, por ejemplo; si esta persona se descuida y utiliza la misma contraseña, será muy fácil para el intruso ingresar a sus cuentas seguras.

- En caso de utilizar certificados digitales, tener en cuenta que el titular de éstos es el responsable de su custodia y conservación. Esto va tanto para el cliente como para el vendedor.
- Bajo ninguna circunstancia comunicar a un tercero la contraseña que permite activar la clave privada de firma. En caso de tener conocimiento o sospecha de compromiso de la clave privada, solicitar inmediatamente a la Autoridad de Certificación la revocación de un certificado. Es muy recomendable estar bien informado del documento de la «*Declaración de Prácticas de Certificación*» emitido por la Autoridad de Certificación.
- Nunca dejar desatendido el ordenador mientras se haya establecido una conexión segura. Es recomendable utilizar protectores de pantalla con contraseña o activar las funciones de bloqueo del terminal (teclado, por ejemplo).
- En caso de utilizar certificados digitales almacenados en una tarjeta criptográfica no dejar ésta conectada al lector del ordenador. Cuando no sea necesario utilizar los certificados se debe extraer la tarjeta aunque se continúen utilizando los servicios del portal.
- Introducir datos financieros sólo en sitios web seguros. Además, el acceso a dichas páginas debe hacerse tecleando directamente la dirección de la banca electrónica en la barra de dirección del navegador.
- Utilizar para sus compras una tarjeta de crédito específica para estos fines con límite de gasto reducido.
- Permanecer atento a todas las novedades relativas al Comercio Electrónico.
- Para aquellos que tengan experiencia comprando y/o vendiendo "en persona"

(por las vías habituales) se podrá hacer uso del sentido común al momento de realizar transacciones vía Internet, lo cual será de gran ayuda.

- Asegurar que se realizan los trámites desde un equipo libre de software malicioso.
- Desconfiar de cualquier correo electrónico que solicite identificación de usuario, contraseña o firma electrónica. Poner este hecho al conocimiento de los responsables del portal.

Es importante asegurarse que en la computadora desde donde vamos a realizar una transacción en el e-commerce no exista software malicioso (Malware), o sea spyware y oportunidades de phishing, entre otros. Por eso debemos disponer de un anti-spyware y una herramienta para navegador anti-phishing. Actualmente, existen soluciones antivirus más completas que vienen con herramientas para tratar todos estos temas además de un conjunto más amplio de Malware. Este punto será introducido más específicamente en la próxima sección bajo el título: "Malware y Comercio Electrónico".

## Malware Y Comercio Electrónico

En uno de los puntos en la última sección, se dio como pauta importante la de realizar las transacciones en el Comercio Electrónico desde un ordenador libre de Malware, pero, ¿Qué es en realidad el malware?

Malware (del inglés malicious software, también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.<sup>21</sup>

Según describe la definición, existe una amplia categoría de este tipo de software. Dicho esto, en la presente sección se llevará a cabo un análisis, plantearán interrogantes y expondrán las soluciones existentes sobre todo aquel software malintencionado que atente directamente contra la seguridad en el Comercio Electrónico.

De esta manera, se considera importante el siguiente Malware:

- ✓ Cookies
- ✓ Keyloggers
- ✓ Pharming
- ✓ Phishing
- ✓ Spyware

---

21 Extraído de: [http://es.wikipedia.org/wiki/C%C3%B3digo\\_maligno](http://es.wikipedia.org/wiki/C%C3%B3digo_maligno)



## Cookies

### ¿Qué Son Y Para Qué Se Usan?

En términos generales, una cookie es un archivo de texto pequeño almacenado en el disco duro de la computadora del usuario que visita una página web. Su invención se debe a las limitaciones propias del protocolo HTTP para mantener información de la navegación del usuario.

Entre los usos más frecuentes de las cookies están: El almacenamiento de nombres de usuario y contraseñas, ofrecer opciones de diseño o contenidos al visitante, e intentos de spyware. En el primer caso ésto provoca que el usuario no tenga que introducir los datos mencionados para cada página del servidor que visita; un ejemplo de este uso es el que otorgan Yahoo y otros clientes de Webmail. En el segundo caso, un ejemplo claro de este uso se ve en iGoogle, que es una página de inicio personalizable la cual permite entre otras cosas agregar Web Feeds y Google Gadgets. El tercer caso se refiere al intento de spyware por parte de agencias de publicidad y otros, mediante la obtención de información sobre *ciertos* hábitos de navegación del usuario, por lo cuál algunos consideran a las cookies como un tipo de malware que atenta contra la privacidad.<sup>22</sup>

Uno de los usos más comunes de las cookies en el Comercio Electrónico es para simular un “carrito de compras”, manteniendo un seguimiento de los productos que el usuario va eligiendo mientras recorre la tienda virtual. También pueden ser usadas para almacenar nombres de usuario y contraseñas, entre otras cosas.

### Problemas Que Pueden Ocasionar A Los Usuarios De Comercio Electrónico

El lector se preguntará:

¿Pueden las cookies atentar, además de la privacidad, contra el robo de identidad? ¿Qué consecuencias traería aparejado?

¿Cuán seguro es el número de identificación que los sitios web emplean para encriptar la información contenida en una cookie?

¿Estamos lo suficientemente seguros de que solamente la información en las cookies será accedida por el servidor que la envió? Si fuese creada y accedida mediante script ¿Cómo puede uno asegurarse de que esa información no caerá en manos indeseables?

### Análisis De Los Interrogantes

Si bien una cookie no identifica a una persona, sino a una combinación de computador y navegador, siempre ofrece pistas a piratas informáticos experimentados (y no tanto), que les permitirán dar con el paradero de la persona a la que pertenece dicha información. Supóngase un caso particular para responder a los interrogantes que se acaban de plantear:

Una familia utiliza un ordenador en común con conexión a Internet; uno de sus miembros, o cualquier otra persona amiga de alguno de ellos, ingresa a un sitio Web de Comercio Electrónico con su nombre de usuario, password, URL, etc.

22 Más información en: <http://es.wikipedia.org/wiki/Cookie> y [http://www.onpei.gob.pe/seguridad/seguridad2\\_archivos/Lib5010/cap0204.htm](http://www.onpei.gob.pe/seguridad/seguridad2_archivos/Lib5010/cap0204.htm)



Esta información será almacenada en una cookie. Hágase de cuenta que el ordenador se encuentra interceptado por algún individuo malintencionado el cual, en este caso, accede a la cookie de manera local; supóngase que ésta, a pesar de estar encriptada, logra ser desencriptada por el individuo quien de esta forma identifica los datos contenidos en la misma. En ese momento el atacante cuenta con los datos privados de aquel usuario que al ingresar al sitio, mediante la URL e introduciendo usuario y contraseña, puede obtener toda la información personal de éste. Estos datos puede que sean útiles al atacante para hacer uso de la Ingeniería Social, con el fin de obtener números de tarjetas de crédito y otra información crítica para luego comprar ocasionando un fraude. Otra alternativa, puede ser que el intruso establezca directamente una sesión a la cuenta particular de la víctima, usando la cookie, sin necesidad de desencriptar la información contenida en la misma.

Ahora bien, supóngase que el atacante no tiene acceso al ordenador cliente (físicamente, o mediante un backdoor, etc.) como en el ejemplo del párrafo anterior, pero sí podría:

- En el proceso de envío de un extremo a otro entre el servidor y el cliente que está navegando, interceptar la cookie mediante sniffing o análisis de tráfico, lo cual es posible realizar sobre sesiones HTTP normales.
- Mediante lo que se llama Cross Site Scripting (XSS)<sup>23</sup>, utilizar el navegador del cliente<sup>24</sup> para ejecutar un segmento de código que reenvíe una cookie a uno o más ordenadores que no deberían acceder a ella. Esta posibilidad es explotada introduciendo un segmento de código en un envío HTML.

El contenido dinámico que han incorporado los sitios Web permite mejorar la experiencia del usuario presentando diferentes salidas dependiendo de sus configuraciones o necesidades (como lo hacen las cookies). Pero este tipo de sitios sufren de una amenaza que no la traen los sitios estáticos: el XSS.

XSS ocurre cuando una aplicación Web obtiene datos de un usuario generalmente bajo la forma de un hiperenlace que posee cierto contenido malicioso. El usuario muy posiblemente clickeará en el link que aparezca en un sitio Web, mensajero instantáneo o al leer información en un foro o correo electrónico. Usualmente el atacante codifica en hexadecimal (u otro sistema de codificación) la porción de código malicioso del link que postea, de manera que sea menos sospechoso para quien lo acceda. Después de que los datos son recogidos por la aplicación Web, una vez que el usuario accedió al link, se crea una página Web de salida de manera tal que parezca el contenido del sitio Web original. Muchos foros, blogs y otras páginas Web, permiten a los usuarios postear links con código html y javascript embebido. Si, por ejemplo, alguien se loguea como “Juan” y lee un mensaje creado por “Pepe”, el cual contiene código malicioso javascript en él, entonces quizás sea posible para “Pepe” *secuestrar*<sup>25</sup> la sesión de “Juan” sólo leyendo su tabla de anuncios (post bulletin board).<sup>26</sup>

23 Más información sobre su funcionamiento: *Hacking Ético*, página 145,

24 Los navegadores modernos permiten la ejecución de scripts recibidos por el servidor (JavaScript, CGI, etc.)

25 Es la traducción del término en inglés “hijacking”. Más información en:

<http://es.wikipedia.org/wiki/Hijacking>

26 Más información en: [http://www.xssed.com/article/11/Paper\\_The\\_Cross\\_Site\\_Scripting\\_XSS\\_FAQ/](http://www.xssed.com/article/11/Paper_The_Cross_Site_Scripting_XSS_FAQ/)

### Respuesta A Las Problemáticas

De esta manera se puede afirmar que existe la posibilidad de que las cookies atenten contra el robo de identidad, siendo las consecuencias de ello muy graves. En secciones anteriores se habló sobre la encriptación de datos y se dejó claro el hecho de la posibilidad de desencriptación de la misma. Tampoco, nunca estamos cien por ciento seguros para pensar que la información personal almacenada en una cookie será accedida únicamente por el servidor que la envió, y si fuese así, tampoco lo estamos en el sentido de que aquél no esté intervenido.

Mientras que los prestadores de Comercio Electrónico sigan delegando parte de su esquema de seguridad a los clientes mediante las cookies almacenadas en los ordenadores de estos últimos, las alternativas de disminución de riesgo deberán ser implementadas por software del lado del cliente.

### Soluciones Existentes

Actualmente los navegadores Web proporcionan opciones de bloqueo, limpieza y filtrado de cookies, que son de hecho soluciones eficientes pero no lo demasiado automáticas y eficaces para los usuarios. Si se habilita la opción “denegar todas las cookies”, existen ciertos sitios que requieren sí o sí que estén habilitadas, y si somos usuarios habituales de éstos, esta opción no es la más adecuada; por otra parte, el hecho de que el navegador pregunte cada vez si el usuario desea aceptar una cookie resulta demasiado tedioso para la mayoría de ellos, los cuales además poseer conocimiento de cuándo una cookie podría resultar peligrosa o no. La limpieza de cookies debe ser también una tarea tediosa, y si bien existe la opción de que se realice cada vez que se cierra el navegador, hay sitios en los cuales nos resulta cómodo el uso de cookies. La existencia de filtros es bastante aceptable pero también requiere de la laboriosidad y la experiencia del usuario para su buen aprovechamiento. Por otro lado, deshabilitar la ejecución de scripts en los navegadores también reduce el riesgo según lo planteado, pero a su vez esta característica que ahora poseen los navegadores modernos facilita mucho otros mecanismos, por lo cual no es del todo una solución efectiva. El uso de HTTPS también ayudaría a evitar la interceptación de una cookie mediante sniffing, pero no un ataque de XSS.

### Soluciones Software Propuestas

En base a lo desarrollado, mi propuesta sería incorporar soluciones software a estos problemas, como ser:

- ✓ Implementación de filtros inteligentes y dinámicos que permitan habilitar o deshabilitar las cookies de determinados sitios utilizando heurísticas.
- ✓ Módulos de control de actividad de acceso a las cookies para determinar que cada servidor que crea una cookie sea éste el que acceda posteriormente a la misma u otro servidor autorizado o del mismo dominio.
- ✓ Sistemas que identifiquen patrones dentro de los scripts antes de que lleguen a ser ejecutados por el navegador para alertar al usuario de la posible existencia de código que pueda poner en peligro la identidad del usuario.

Sería importante destacar que una implementación más controlada se lograría si los servidores que contienen sitios de Comercio Electrónico pueden obviar el uso de las

cookies por el lado del cliente e implementar mecanismos de seguridad solamente en el extremo del prestador de servicios, pero debido a las limitaciones actuales de los protocolos de comunicación esto no es utilizado por los proveedores habitualmente.

## Keyloggers

### ¿Qué Son Y Para Qué Sirven?

Un keylogger (registrador de teclas) es una herramienta [...] que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero y/o enviarlas a través de Internet.<sup>27</sup>

Uno de sus usos menos deseables es el de ocasionar el robo de cuentas de usuario y contraseñas, entre otras cosas, lo que atenta contra la confidencialidad. Debido a esta razón, también se considera dentro de la categoría de Malware.

No existe razón alguna para pensar que puedan llegar a ser útiles en el ámbito del Comercio Electrónico, sino es para obtener información legítima de manera, podría decirse, ilegal.

### Tipos De Keyloggers

El keylogging se realiza mediante herramientas software o hardware. Ya que se habla de Malware, se hará mención únicamente a las herramientas software. Así, dentro de esta categoría tenemos keyloggers<sup>28</sup>:

- ✓ Basados en núcleo: Son los más poderosos pero a la vez los más difíciles de programar. Éstos residen en el nivel del núcleo del sistema operativo y son prácticamente invisibles. Pueden acceder a todas las teclas pulsadas sobre el teclado.
- ✓ Enganchados: Estos keyloggers enganchan el teclado con las funciones que proporciona el sistema operativo.
- ✓ Otros métodos: Estos otros utilizan funciones específicas que requieren revisar de manera constante el estado de las teclas, lo que puede aumentar sensiblemente el uso del CPU e incluso no registrar algunas pulsaciones.

### Problemas Que Pueden Ocasionar A Los Usuarios De Comercio Electrónico

Para el caso del Comercio Electrónico representa una mayor amenaza que las cookies, por el hecho de que quien acceda a sus cuentas en sitios de compra online desde una máquina infectada, no sólo expondrá sus datos (como nombre de usuario y contraseña), sino que todo aquello que teclee incluyendo números de cuentas bancarias, tarjetas de crédito y cualquier otro tipo de datos de importancia crítica. La existencia de keyloggers en ordenadores es una de las amenazas menos deseadas de aquellos usuarios que compren por Internet, y la razón está más que clara.

### Soluciones Existentes

He aquí algunas soluciones “caseras” y otras de software para poder determinar la

27 Extraído de: <http://es.wikipedia.org/wiki/Keylogger>

28 <http://www.alegsa.com.ar/Dic/keylogger%20por%20software.php>

existencia de keyloggers en nuestro sistema o evitar el funcionamiento de los mismos si los hubiere. Ciertas soluciones, que se procede a enumerar, pueden ser aplicadas de manera simultánea para reducir el riesgo de infección<sup>29</sup>:

- Algunos keyloggers programados por software registran cada una de las teclas pulsadas agregándolas a un fichero *log* por cada vez que se presiona una tecla. Si bien este evento no es una carga relevante para la mayoría de los procesadores actuales, si se llegase a determinar un gran número de pulsaciones de teclado a la vez, puede que se note cierta lentitud en el procesamiento que no resulte usual.
- En Windows se puede acceder al Administrador de Tareas (mediante ctrl + alt + supr) para analizar los procesos activos y determinar la existencia de keyloggers. Obviamente, un keylogger tendrá un identificador de proceso poco común, así que si no se conoce cuáles de ellos se ejecutan cotidianamente en nuestro sistema, entonces se pueden buscar dichos identificadores en Internet, utilizando por ejemplo Google, Yahoo, etc., de tal manera que podamos saber de qué se trata. Otros procesos quizás se encuentren ocultos y puedan ser detectados utilizando herramientas *anti-rootkit*.
- Puede haber entradas en el registro de Windows que activen un keylogger cada vez que se inicia una sesión o el sistema.
- Existe software Anti-Spyware que detecta muchos keyloggers y los elimina.
- Supongase que ninguno de los métodos de búsqueda y eliminación anteriores dio indicio de la existencia de algún tipo de keylogger, entonces lo que se puede hacer es prevenir que la información que éste almacene sea transmitida sobre la red utilizando algún filtro de Firewall.
- Otra forma de evitar dar acceso a la red a un keylogger es utilizando los Monitores de Red, que alertarían al usuario siempre que un servicio intente realizar alguna conexión.
- También se puede engañar a los keyloggers de diversas formas, como por ejemplo: se puede alternar escribiendo en una ventana un carácter y luego otro en otra, o mover el cursor mientras se tecléa haciendo que el keylogger detecte las combinaciones de teclas en el orden incorrecto, o también se pueden usar menús contextuales para copiar y pegar trozos de texto o caracteres para no tener que escribirlos y que sean así detectados..

Además de estas soluciones, se encuentra algo más específico. Se trata del *Software Anti-keylogging*. Este software, como su nombre lo indica, está dedicado exclusivamente a la detección y eliminación de keyloggers; algunos Anti-keyloggers están basados en firmas y otros, más sofisticados, no dependen de ellas sino que son soluciones basadas en algoritmos que detectan comportamientos en base a patrones, exponiendo a este tipo de Malware y deshabilitándolo instantáneamente. Los algoritmos mencionados tienen la capacidad de brindar protección incluso ante keyloggers hechos de manera personalizada, que son muy peligrosos, y para los cuales tardarían en salir firmas actualizadas para su detección, como sucede por

---

29 Extraído y adaptado de: <http://es.wikipedia.org/wiki/Keylogger>

ejemplo con los virus y troyanos.<sup>30</sup>

### Soluciones Software Propuestas

Según la perspectiva del autor, las soluciones existentes ya enumeradas resultan bastante eficientes y efectivas. Aunque se considera que lo más adecuado sería disponer de una solución software que se ocupe de la detección inmediata y en tiempo real de este tipo de Malware. La base para la operación de esta solución es utilizar un *algoritmo de aprendizaje supervisado determinístico*: el cual recibe como entrada el valor correcto para determinados valores de una función desconocida y debe averiguar cuál es la función y aproximarla. [Russell y Norvig, 2006]. Para el caso particular planteado, la función desconocida vendría a ser el algoritmo de detección perfecto (desconocido), por así decirlo, y los valores correctos de la función que se dan como entrada serían las firmas. Además de esto, también es necesario contar con un mecanismo de inferencia que correlacione los datos de entrada modificando el algoritmo de detección para mejorarlo. Por otro lado, dado un conjunto de firmas, algunas pertenecerán al llamado *conjunto de entrenamiento*, quienes ayudarán en la mejora del algoritmo; mientras que otras estarán incluidas en el *conjunto de prueba*, con las cuales se comprobará la eficiencia del algoritmo; luego, las firmas incluidas en este último grupo pasarán a ser de entrenamiento y se incorporarán nuevas firmas hasta ir logrando mejores resultados.

## **Pharming**

### ¿Qué Es?

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.<sup>31</sup>

### Tipos De Ataque Pharming

Un ataque pharming puede realizarse directamente a los servidores DNS, afectando a todos los usuarios, o bien atacando a ordenadores de escritorio (llamado *pharming local*) mediante la modificación del fichero "hosts", que relaciona unívocamente direcciones IP con nombres de sitios Web para resolverlos en forma local, y que está presente en cualquier equipo que funcione bajo Windows, Unix o Mac, entre otros.<sup>32</sup>

Si bien tanto el pharming local como el DNS perjudican al cliente, se plantearán soluciones para el primero, ya que, como en todos los casos de Malware tratados en el trabajo, la idea es ocuparse de la seguridad del lado del cliente y qué se puede hacer desde su lado para disminuir el riesgo de ataque.

<sup>30</sup> Más información en: <http://www.anti-keyloggers.com/>

<sup>31</sup> Extraído de: <http://es.wikipedia.org/wiki/Pharming>

<sup>32</sup> Más información en: <http://www.psicofxp.com/forums/seguridad-informatica.47/522258-clonacion-de-sitios-web-comprometiendo-confidencialidad.html>

### Principales Usos Y Problemas Que Ocasiona En Comercio Electrónico

Este tipo de ataque se suele utilizar como **medio** para la concreción de otros ataques como ser el phishing<sup>33</sup> (que será explicado en el próximo apartado), redirigiendo el nombre de dominio de una entidad de confianza a una página Web con apariencia idéntica, pero fraudulenta, con el fin de obtener datos críticos de un usuario.

Si bien no compromete de manera directa la información del usuario de Comercio Electrónico, el hecho de representar un medio para facilitar otros ataques que sí lo harán, es condición suficiente para incluir dicha amenaza en la categoría de Malware.

Puede, por ejemplo, ocurrir que mediante algún tipo de spyware se conozcan las preferencias y los sitios por donde navega un usuario informando al atacante, el cual, conociendo los intereses del este usuario y sabiendo que compra en alguna tienda virtual, envíe una invitación a su correo electrónico o mensajero, engañándolo con algo que resulte de su interés (algún video, tarjeta electrónica, etc.) para que, mientras tanto, se ejecute de manera silenciosa por medio del navegador un script que modifique el fichero "hosts"<sup>34</sup> de su máquina para redirigirlo a una página de phishing la próxima vez que éste ingrese a su sitio Web de compras online. Otra forma de infección, aún más común quizás que la anterior, es a través de un *troyano*, un tipo de Malware que consta de fragmentos de código que se ocultan dentro de programas y/o archivos de datos, efectuando enmascaradamente alguna acción maliciosa [Graziosi, 2007], como ser en este caso la modificación del fichero "hosts". Para este caso particular, el troyano vendría a ser el medio para efectivizar un ataque de pharming, y el pharming, en consecuencia, otro medio para un ataque de phishing.

### Soluciones Existentes

En el mercado se encuentran soluciones anti-pharming para la protección de servidores DNS como así también pequeñas aplicaciones de escritorio o add-ons para los navegadores Web con el objeto de proteger al usuario del *pharming local*. Éstas últimas son soluciones orientadas al fin y no al medio, es decir, a detectar y eliminar páginas de phishing utilizando generalmente una base de definiciones. Se puede asegurar más el sistema deshabilitando la función de ejecución de scripts del navegador o disponiendo de un antivirus actualizado que sea capaz de detectar y eliminar troyanos.

Todas estas soluciones pueden implementarse a la vez disminuyendo la posibilidad de este tipo de ataques.

Por otro lado, no hace mucho tiempo, se ha descubierto una vulnerabilidad inherente al protocolo DNS que permitía falsificar las respuestas DNS, y por tanto redireccionar el tráfico.<sup>35</sup> Ésto puede remediarse mediante el uso de soluciones del tipo **opendns**<sup>36</sup>, que se encuentra actualizado para protegernos de esta vulnerabilidad,

33 Algunos autores consideran al pharming directamente como una evolución del phishing:

<http://www.laflecha.net/canales/seguridad/articulos/pharming/>

34 Para tal motivo se debe tener permisos de Administrador

35 Más información en: <http://seguinfo.blogspot.com/2008/07/los-detalles-de-la-vulnerabilidad-en-el.html>

36 Más información en: <http://www.opendns.com/>



además del phishing, dando a su vez la opción para el filtrado de contenidos Web y bloqueo de dominios individuales, entre otras cosas.

### Soluciones Software Propuestas

Lo ideal es comenzar protegiendo el medio. Es decir, como se expuso con anterioridad, la generalidad de los ataques de pharming se realizan directamente al archivo "hosts", presente en los sistemas operativos comúnmente utilizados por la mayoría de los usuarios. ¿Cómo se podría evitar la modificación y/o agregación de entradas no legítimas a tal fichero? Considero que lo ideal sería desarrollar un módulo software que implemente un proceso demonio para determinar qué cambios son deseables, de manera automática y en tiempo real, según la *base de conocimiento*<sup>37</sup> de la aplicación. Dicho conocimiento se refiere al estado y las modificaciones que generalmente sufre el fichero "hosts". El software también podría tener la capacidad de aprender, incorporando las experiencias buenas y malas para deducir y tomar acciones mejores y más óptimas cada vez que sea necesario.

Otra solución podría ser la creación de una aplicación que compare la actividad de dos o más servicios DNS y sólo permita al usuario el acceso a la información cuando coincidan las respuestas a la petición de los DNS incluidos. Supóngase que esta aplicación está corriendo en un sistema y se desea ingresar a un sitio Web: [www.clarin.com](http://www.clarin.com), entonces si los servidores DNS que están configurados en la aplicación responden con la misma dirección IP, se permitirá ingresar; de lo contrario, si las respuestas no son las mismas, se puede delegar al usuario la toma de decisiones, o bien determinar de manera automática mediante un método o comparando con la información de otros DNS, cuál es la página original.

## **Phishing**

### ¿Qué Es Y Con Qué Fin Se Utiliza?

Se comienza definiendo un término necesario para comprender el significado de phishing: la *Ingeniería Social*. En el campo de la Seguridad Informática, Ingeniería Social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos<sup>38</sup>; aun más fácil: es una técnica para convencer a la gente de entregar información. El phishing es una técnica de Ingeniería Social usada para engañar a los usuarios con el fin de obtener o adquirir en forma fraudulenta sus contraseñas, nombres de usuario u otro tipo de información personal. El phishing es un delito encuadrado dentro del ámbito de las estafas en el cual, el estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.<sup>39</sup>

### Principales Usos Y Problemas Que Ocasiona En Comercio Electrónico

Sin duda alguna, los casos de phishing van en incremento tanto en Argentina como en el mundo entero. Estos ataques van dirigidos a todo tipo de sitios Web: aquellos con fama de ser clonados, como ser a entidades bancarias, que bien se puede decir

37 Nótese que se está haciendo referencia a un Sistema Inteligente. [Russell y Norvig, 2006]

38 Extraído de: [http://es.wikipedia.org/wiki/Ingenier%C3%ADa\\_social\\_\(seguridad\\_inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica))

39 Extraído de: <http://es.wikipedia.org/wiki/Phishing>



representan la mayoría de los casos, u otros poco conocidos. El phishing tiene por objetivo obtener información crítica de los usuarios que le permitan llevar a cabo fraudes al phisher, en base a lo cual se puede razonar y determinar en qué casos cada vez que recibimos un email, un link por medio del mensajero, etc. se es víctima del phishing, siendo que al ingresar a tales sitios se pida rellenar datos sensibles.

mercado Libre

MercadoLibre asegura la confidencialidad de los datos aquí suministrados. Te invitamos a revisar nuestras [Políticas de Seguridad](#)

Verifige Secured

### Datos Personales

Nombre\*:  Apellido\*:

País\*:  País:

Estado\*:  Ciudad\*:

Teléfono\*:  Extensión:

Teléfono 2: (opcional)  Extensión:

\*Datos obligatorios

→ MercadoLibre no vende o alquila tu información personal a terceros sin tu consentimiento. Conoce nuestras [Políticas de Privacidad](#)

TRUSTe

### Datos de Usuario en MercadoLibre

Seudónimo\*:

Con este seudónimo te identificas en la comunidad de MercadoLibre.

Clave\*:

La clave debe tener entre 6

E-mail\*:  Repetir e-mail\*:

Utilizaremos este e-mail para confirmar.

☒ Acepto Los Terminos y Condiciones de MercadoLibre.

Ingresa el código que observas en la imagen\*:

Indicarlo mayúscula o minúscula.

Continuar

\*Datos obligatorios

TRUSTe

Cotidianamente se descubren nuevos intentos de phishing. Un caso de interés es el de Mercado Libre. A continuación se pone a disposición una imagen de la página clonada<sup>40</sup>: Como se apreciará, al completar este formulario haciendo clic en “Continuar”, se está entregando datos importantes (información) al atacante. El usuario no se percatará, ya que el resultado de la solicitud será un error de página, un aviso de caducidad de cuentas, o simplemente no habrá aparente respuesta. De esta manera se determina que los usuarios de Comercio Electrónico no están exentos de recibir este tipo de ataque de Malware.

### Soluciones Existentes

Algunas recomendaciones para evitar ser atacados mediante phishing son<sup>41</sup>:

- Cada vez que se ingrese a un sitio y se tengan que introducir datos que

40 Más información en: <http://blogs.eset-la.com/laboratorio/2008/07/07/phishing-todos-gustos/>

41 Más información en: <http://blogs.eset-la.com/laboratorio/index.php?s=phishing>

puedan resultar comprometedores, revisar la URL de manera tal que se trate del sitio original.

- Si se tiene conocimiento sobre HTML, PHP, u otro lenguaje similar, en el código fuente de la página puede verse la modificación realizada para que cuando al hacer clic en el botón “continuar”, “enviar”, etc. se envíe la información al atacante.
- Puede que se reciban intentos de ataque phishing a través del correo electrónico. Es recomendable que el usuario se detenga a observar posibles errores de ortografía y determine, usando el sentido común, si es posible que la entidad suela hacer el tipo de peticiones realizada a través de tal medio. Ante la duda, remitirse al sitio de confianza antes de realizar cualquier operación.
- Algunos navegadores Web, los más modernos, traen incluidas funcionalidades anti-phishing que muestran una alerta cuando se sospecha que alguna página Web intenta obtener datos personales o financieros bajo falsos pretextos. Este pequeño software suele utilizar una combinación de algoritmos e informes sobre páginas phishing de una o diversas fuentes. Cuando un navegador no trae dicha funcionalidad, puede incorporársele como plug-in.

#### Soluciones Software Propuestas

Como solución ante esta amenaza se propone desarrollar una aplicación que tenga incorporada una larga lista de sitios Web, originales y propensos a recibir ataques de phishing, junto con su *mapa de diseño visual*. De esta manera cada vez que se ingrese a un sitio, la aplicación hará una búsqueda en su base de datos e intentará identificar páginas con un alto grado de parecido en el diseño pero con ciertas anomalías en el mismo. La base con los mapas visuales de cada página Web deberá ser actualizada cada vez que se hagan modificaciones en el diseño original de alguna de ellas. Así, la única forma de tener la aprobación de la aplicación en el proceso de comparación será con la casi total diferencia, o bien con la coincidencia en un 100% entre los mapas de diseño visual (patrones) y la página visitada. Para la programación de los algoritmos de detección de patrones podría resultar útil el empleo de técnicas usadas en software de reconocimiento facial. Como un plus, ésta solución puede ser parte de un servicio que se le preste a aquellos portales que deseen aumentar su seguridad, haciéndose menos vulnerables al phishing y ganándose la confianza del cliente por ello.

Otra solución posible podría estar basada en el análisis del código fuente de las páginas que se deseen, para determinar cuáles resultarían ser peligrosas. Este análisis podría ser realizado por un algoritmo que envíe ciertos datos al formulario de la página y, que en base a los resultados o acciones devueltos por ésta, determine la autenticidad del sitio Web bajo análisis.

Por último, es interesante el hecho de que pueden añadirse en otras capas soluciones ya existentes a las propuestas para disminuir el riesgo de estos ataques, sin el peligro de que entren en conflicto.

## Spyware

### ¿Qué Es Y Para Qué Se Usa?

El spyware es el conjunto de programas informáticos que se instalan en una computadora personal para interceptar o tomar control parcial sobre la interacción del usuario con la computadora, a veces, sin el consentimiento informado del mismo.<sup>42</sup>

El uso más común es el que hacen las compañías publicitarias, que lo instalan en la computadora de uno sin ser avisados. De acuerdo a la política de privacidad de tales compañías, no se recolectarían datos sensibles o identificatorios del sistema afectado, el cual a su vez permanecería anónimo. A pesar de ello, siempre existe el hecho de que habrá instalado en nuestro ordenador un servidor que estará enviando información acerca de nosotros y nuestros hábitos de navegación hacia un destino remoto desconocido.<sup>43</sup>

### Composición

En términos técnicos, el spyware puede ser dividido en dos partes de software que se juntan para formar un solo paquete [Post, 2003]:

1. La funcionalidad de núcleo, que es la parte visible y útil para el usuario, y
2. La funcionalidad de recolección de información, que recibe, mantiene, monitorea y envía en segundo plano cierta información sobre el usuario y/o la computadora.

### Problemas Que Ocasiona A Los Usuarios De Comercio Electrónico

Supóngase que Juan instala un reproductor multimedia en su ordenador el cual promete buen desempeño, por así decirlo, como lo promociona el *editor de spyware*<sup>44</sup>. Esta persona quizás deba completar un formulario con sus datos personales y demográficos para concluir el proceso de registración. Luego, Juan comienza a utilizar el programa, notando su aparente elevado desempeño frente a otros, lo cual le produce una grata satisfacción. Así, cada vez que él inicia la aplicación, se le presentan una serie de publicidades de las cuales ciertas son de su interés y ciertas otras no lo son. Cada vez que Juan ingresa a alguno de estos hipervínculos, el navegador notifica al editor de spyware, quien se ocupa de construir un perfil de acuerdo con la información recopilada. De esta manera, se le irán presentando a Juan los anuncios que son probables de estar en su campo de interés.

Como se comentó recién en el ejemplo, y en puntos anteriores, las empresas a menudo utilizan el spyware para obtener información de los usuarios con la finalidad de realizar estadísticas, lo cual en la mayoría de los casos se encuentra establecido en la licencia de dichas aplicaciones spyware. Pero, los detalles sobre las preferencias de los usuarios a la hora de comprar o sitios comúnmente visitados, pueden ser recibidos y/o vistos por alguien que no debería y cuyas intenciones sean

42 Adaptado de: <http://en.wikipedia.org/wiki/Spyware>

43 <http://www.spychecker.com/spyware.html>

44 Del inglés "Spyware publisher", es la entidad que se encarga de recibir la información del usuario y procesarla para algún fin determinado.

las de ocasionar fraude (como lo visto en el caso de pharming).

Entre las formas más comunes de contraer este tipo de Malware se hallan<sup>45</sup>:

- Visitar sitios Web que ejecuten código malicioso sin nuestra autorización (ActiveX, JavaScript, cookies).
- Dentro de un virus o troyano.
- Ocultos dentro de *freeware* (programas gratuitos) como ser utilidades de descarga de ficheros, navegadores Web, juegos, reproductores de medios, software de contabilidad, etc.
- La descarga de ciertos archivos en programas P2P (Emule, Azoreus, Ares, etc.)
- Incluso los sitios confiables pueden contener banners que inciten a la descarga de spyware, como ser los hotbar.
- Existen ciertas aplicaciones, conocidas como *rogue* (pícaras), que aparentan ser de seguridad pero contienen este tipo de Malware.

Cualquiera sea la forma o medio mediante el cual se incorpore spyware al sistema, su modo de operación será similar. Lo que sí cambia es la naturaleza de la información que cada tipo de spyware toma o recoge del sistema donde se instala. [Post, 2003]

Algunos síntomas de infección con spyware pueden ser: el cambio de la página de inicio del navegador, aparición de ventanas pop-ups incluso sin estar conectados y sin tener el navegador abierto, barras de búsquedas de sitios o botones que aparecen en la barra de herramientas del navegador y que no se pueden quitar, navegación por Internet lenta, etc.<sup>46</sup>

### Soluciones Existentes

Primero que todo, es mejor prevenir que curar, así que el primer consejo es tratar de evitar el spyware tomando como base los puntos ya enumerados. A pesar de ello, siempre de alguna manera este Malware va a lograr ingresar al sistema, problema para el cual la medida más común a tomar es la instalación de un software antispyware auténtico<sup>47</sup> basado en definiciones para su detección y posterior eliminación. Soluciones más completas añaden la funcionalidad de detener spyware en *puntos de enlace*.<sup>48</sup>

### Soluciones Software Propuestas

Como se expuso en puntos anteriores el spyware es muy variado y la manera en que cada uno recupera la información es muy diversa: algunos recuperan ciertos datos de utilidad que otros no. La dificultad quizás de implementar soluciones más efectivas del lado del cliente se deba justamente a que deben integrarse muchos conocimientos y plantearse todas las posibles formas de operar del spyware. Una vez que se tenga esta información, se debería mediante alguna técnica de inducción

45 Más información en: <http://blogs.eset-la.com/laboratorio/index.php?s=spyware>

46 <http://www.ylos.com/spa/item/spyware.html>

47 Se debe tener cuidado con las aplicaciones Rogue.

Más información en: <http://blogs.eset-la.com/laboratorio/index.php?s=spyware+rogue>

48 <http://www.pergaminovirtual.com.ar/revista/cgi-bin/hoy/archivos/2005/00000728.shtml>

ver cómo se podría generalizar todo lo recabado y así obtener conclusiones que lleguen a producir resultados interesantes en el desarrollo de soluciones software anti-spyware.

Sin embargo, puede disminuirse el uso del spyware debido al no conocimiento de su presencia en aplicaciones que lo contienen. Esto se podría llegar a lograr si, de parte de los desarrolladores, hubiese una forma más fácil de indicar al usuario que está por instalar un software que contiene spyware. Una opción sería mediante una ventana de diálogo, en vez de presentarlo "oculto" dentro del texto de licencia, cuya lectura en la generalidad de los casos es obviada por los usuarios.

## Resumiendo: Guía Rápida Para Comprar En Internet - Ejemplo

Aquí se da un ejemplo de cómo proceder para comprar en Internet. Ésto es de manera personal, y espero le sea útil al lector.

Pasos:

- 1) Asegurar el ordenador antes de utilizarlo, para esto se pueden tomar los recaudos indicados en las secciones dedicadas a la "Seguridad En Relación Al Cliente" y "Malware y Comercio Electrónico". Es indispensable para ésto que sea entonces un ordenador donde el usuario pueda tener un control total sobre el mismo, siendo en todos los casos no recomendable realizar esta actividad desde equipos de uso público como cibercafés.
- 2) Tener bien claro qué es lo que se quiere comprar: si la cosa es usada o nueva, las características, la marca, y el límite de dinero que se está dispuesto a gastar, etc. Yo opto por comprar un router con Hub/Switch para 4 entradas RJ45 porque sólo quiero tener una máquina saliendo a Internet. Con 4 entradas puedo conectar más máquinas en el futuro. También quiero que tenga un Firewall decente para uso hogareño, que sea multipuesto, que tenga acceso seguro de alta velocidad, soporte VPN múltiple, SNMP, compatible con USB 1.1 y Ethernet. Además, quiero que sea de una marca reconocida. No quiero gastar más de U\$S70 incluido costos de envío.
- 3) Ingresar a un sitio de confianza para buscar el artículo deseado. Puede ser uno B2C o C2C, es decir, una página de un proveedor o vendedor específico que venda a través de Internet u otra como Mercado Libre donde haya muchos vendedores. Yo me decidí por Mercado Libre; ingresé con mi usuario y busqué "ADSL Router".
- 4) Buscar el artículo que mejor responda con la idea de lo que se quiere comprar (vistazo general). En mi caso, obtuve muchos resultados (<http://listado.mercadolibre.com.ar/adsl-router>). Entre ellos vi: D-LINK ROUTER MODEM ADSL ETHERNET + USB Mod. DSL-522B NUEVO, de U\$S 64. Así que decidí entrar para ver más información.
- 5) Ver los detalles del artículo y si es necesario consultar más al vendedor. Leyendo un poco las características del producto me encontré con que tiene todo lo que yo buscaba (o al menos la mayoría de las cosas, pero tiene lo más importante).
- 6) Investigar al vendedor. Aquí se tendría que poner en práctica lo visto en la

sección "Seguridad en relación al vendedor". En mi caso encontré que este vendedor tiene 100% de calificaciones positivas y tiene 7500 artículos vendidos; por ésta y otras razones he decidido comprarle. Ésta es la página del producto:

[http://articulo.mercadolibre.com.ar/MLA-30729571-d-link-router-modem-adsl-ethernet-usb-mod-dsl-522b-nuevo-\\_JM](http://articulo.mercadolibre.com.ar/MLA-30729571-d-link-router-modem-adsl-ethernet-usb-mod-dsl-522b-nuevo-_JM). Ésta es la página con las estadísticas del vendedor: <http://www.mercadolibre.com.ar/jm/profile?id=7055243>.

7) A continuación, algunos consejos resumidos para antes de comprar<sup>49</sup>:

- **Revisar el historial del usuario (vendedor).** ¿Cuántas calificaciones positivas y negativas tiene, en qué transacciones participó y cuál fue el resultado final de las mismas?
- Profundizar el conocimiento sobre aquello que se va a comprar antes de confirmar la oferta. Comparar los artículos que ofrecen diferentes usuarios y **hacer todas las preguntas al vendedor que se necesiten**, por ejemplo acerca de costos y métodos de envío, la garantía y posible devolución.
- Leer en detalle la información publicada y prestar especial atención a:
  - toda la información ofrecida
  - las fotos del artículo
  - los diferentes tipos de pago y de envío ofrecidos
- Si el precio del producto es significativamente menor al precio sugerido de venta al público, se deben tomar recaudos especiales a la hora de pactar el envío y el pago.

8) Decidir la Compra. Recomendaciones para después de decidir la compra:

- Si el vendedor lo acepta, es recomendable **utilizar servicios de pago seguros, sobre todo en operaciones a distancia y/o de montos importantes**. La mayoría de las páginas de Comercio Electrónico C2C incluyen este tipo de servicios.
- **Sólo se hace un depósito o consignación de dinero en un banco si la contraparte inspira confianza.**
  - **Siempre cerciorarse de que los datos del vendedor coincidan con los de su cuenta.**
- No utilizar servicios de transferencia de dinero que no permitan verificar la identidad de la contraparte.
- Utilizar el sentido común a la hora de planificar con la contraparte el intercambio.
- Asegurarse que la contraparte tenga un teléfono fijo donde poder contactarlo ante cualquier duda.
- Cuando sea posible examinar bien al artículo antes de realizar el pago final.

49 Extraído y adaptado de: <http://guia.mercadolibre.com.ve/compra-seguro-mercadolibrecom-19767-VGP>

- 9) Limpiar todo rastro de la transacción realizada. Limpiar toda la información posible en el navegador usado para la transacción y volver a repetir procedimiento de aseguramiento del ordenador.



## Conclusión

Se considera haber dado un panorama bastante completo de lo que es Comercio Electrónico para aquellos que recién se inician, incluidas medidas de seguridad orientadas a quienes compran. En este punto el usuario (comprador) tiene los conocimientos necesarios para distinguir los distintos tipos de sitios (B2C, C2C, etc.) que definen las formas de negociar en Internet, está enterado de cómo elegir un portal confiable, cómo evaluar un vendedor, qué consideraciones debe tener en cuenta con respecto al canal de comunicación, y qué recaudos del lado del cliente (en su ordenador).

El análisis realizado sobre cierto Malware, que se consideró en un principio vinculado con el Comercio Electrónico, llevó evidentemente a constatarlo. De hecho, claro se vio que, en muchos de los ejemplos e interrogantes planteados, su influencia sobre la actividad comercial electrónica resultó elevada. Se espera también, que las soluciones planteadas tengan aplicación en el campo de la industria del software pudiendo contribuir a mejorar la seguridad de los usuarios de este tipo de transacción.

Para terminar, el estudio hecho a lo largo del trabajo demuestra que no es totalmente inseguro el hecho de comprar por Internet, pero sí hemos de saber que hay muchas implicancias a tener en cuenta. En definitiva, como en todo, existe un riesgo, un riesgo que podemos mitigar siguiendo pautas de seguridad, pero que si las descuidamos y no hacemos frente a nuevas amenazas, podemos todos caer en las oscuras garras del fraude digital.

## Bibliografía

- **[Graziosi, 2007]** Mauro Graziosi. *Cátedra Seguridad de la Información*. UTN Facultad Regional San Francisco. 2007.
- **[Coudert y otros, 2007]** Fanny Coudert, Ana Marzo Portera, Yolanda Navalpotro, Cristina Almuzara Almaida. *Estudio práctico sobre la protección de datos de carácter personal*. Editorial Lex Nova, 2007.
- **[Tori, 2008]** Carlos Tori. *Hacking Ético*. Astroianni Impresiones. 2008.
- **[Russel y Norvig, 2006]** Stuart Russell y Peter Norvig. "Capítulo 18". En: *Inteligencia Artificial – Un Enfoque Moderno*. Ed. Prentice Hall, 2006.

## Weblografía

- <http://www.cmt.es/>
- <http://www.cace.org.ar/>
- <http://es.wikipedia.org/>
- <http://www.wikilearning.com>
- <http://www.glosariointernet.com>
- <http://www.seguridadenlared.org>
- <http://www.programacionweb.net>
- <http://arte.mundivia.es/>
- <http://www.alegsa.com.ar/>
- <http://www.anti-keyloggers.com/>
- <http://www.psicofxp.com/forums/>
- <http://blogs.eset-la.com/laboratorio/>
- <http://seguinfo.blogspot.com>
- <http://www.panamacom.com/Seguridad>
- <http://www.liderempresarial.com>
- <http://guia.mercadolibre.com.ve>
- <http://www.profeco.gob.mx/>

## Papers

- **[Post, 2003]** André Post. *The Dangers of Spyware*. 2003  
<http://securityresponse.symantec.com/avcenter/reference/dangers.of.spyware.pdf>
- admin@cgisecurity.com. *"The Cross Site Scripting FAQ"*.  
<http://www.cgisecurity.com/articles/xss-faq.txt>