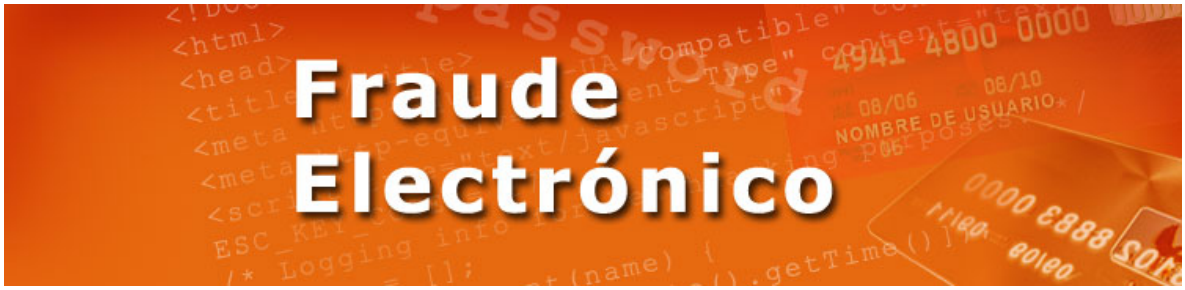
PUNTO SEGURIDAD, SEGURIDAD EN TIC | NÚMERO 2 | AGOSTO 2009 | *ISSN EN TRÁMITE* | REVISTA BIMESTRAL



Javier Ulises Santillán Arenas
Sergio Andrés Becerril López

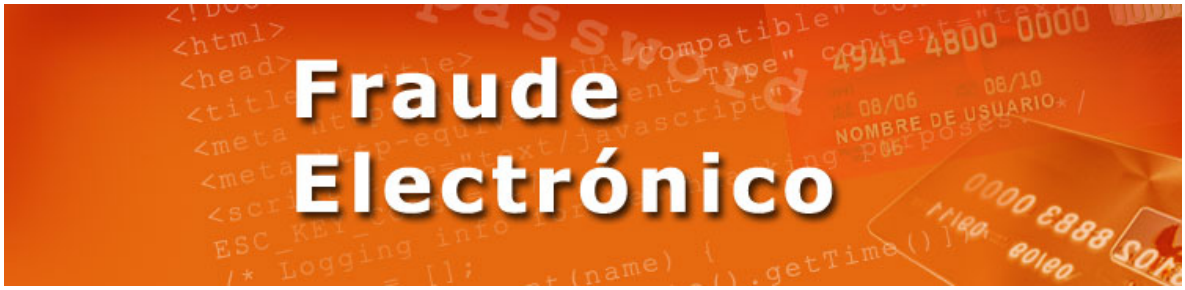
Según las últimas encuestas[1], más del 40% de los usuarios de Internet en México utilizan alguna forma de comercio electrónico. Esto incluye, aunque no de forma exclusiva, compras por Internet, banca en línea, pago de servicios intermedios de transferencias monetarias, etc. Y es que, afrontémoslo: hoy en día es mucho más sencillo realizar nuestras operaciones monetarias con unos cuantos clicks, evitando largas filas de banco, tráfico, etc. Lo que es más, cada vez estamos dispuestos a gastar más en estas transferencias, cuyos rangos van desde los $400 hasta los $1000 en promedio por compras personales, y desde $500 hasta $3000 en compras de negocio. En definitiva, es un área de gran crecimiento y oportunidad de negocio.

Lamentablemente, como todas las áreas de rápido crecimiento y pronunciado interés en la población en general, estamos propensos a ataques por parte de maleantes. Nuestra información financiera es muy valiosa, ya sea para que alguien realice una compra con nuestra tarjeta, o para utilizarla como identificación para procesos más complicados (y, usualmente, mucho más nefastos). En los últimos años, a la par con el crecimiento de Internet y el comercio electrónico, hemos visto un surgimiento de toda una economía *underground* en donde nuestra información es intercambiada, comprada y vendida al mejor postor – y las ganancias no son pocas. Más de la mitad de la información que se comercia son datos financieros, ya sea información de tarjetas de crédito o información de cuentas bancarias en línea, completas con nombres de usuario y contraseñas, y con ganancias de varios miles de dólares. Como se ve, el incentivo para robar esta información es bastante grande.

¿Qué se roban?

Como ya mencionamos, la información más fácilmente utilizable es la más valiosa, y por consiguiente la más buscada. Entre la principal información que buscan los maleantes se encuentran los números de tarjeta de crédito (en conjunto con la información periférica necesaria, como el código de 4 dígitos adicional) que permiten a los maleantes realizar cargos a nuestro nombre, no solo para adquirir mercancías, sino también para suplantar nuestra identidad a la hora de registrarse en algún sitio u organización.

Los propósitos de esto son, a veces, mucho peor que algunos pesos perdidos: el famoso caso de Landslide (1999-2001) mandó a la cárcel a un buen número de personas cuyas tarjetas fueron utilizadas para establecer sitios de pornografía infantil, por ejemplo. Aunque hasta el día de hoy existen apelaciones y los inocentes son (lentamente) liberados, el problema fue gigantesco para los involucrados.



En segundo lugar, los maleantes buscan hacerse de la información de acceso a los sistemas de banca electrónica; esto es, nuestros nombres de usuario y contraseñas. Algunos bancos ya han tomado medidas al respecto (utilizando los famosos 'tokens[1]'), sin embargo todavía existen servicios resguardados únicamente por contraseñas. Esta información es notablemente más difícil de encontrar, y por tanto más valiosa: una sola cuenta de acceso puede ser vendida en $1000 USD, por ejemplo. Con esta información los atacantes pueden acceder a una gama mayor de servicios; una cuenta bancaria les permite realizar movimientos de transferencias (por ejemplo, para lavado de dinero), sin mencionar la obvia razón de vaciado de cuentas.

¿Cómo lo obtienen?

Lamentablemente, los atacantes tienen una amplia gama de opciones para obtener nuestra información. Se valen de engaños (*phishing*, *pharming*), espían nuestras actividades (*spyware*) y, en algunos casos incluso nos atacan directamente (gusanos, virus) con tal de conseguir lo que buscan.

Por supuesto, esto solo describe una forma de obtener la información. Es muy probable que los atacantes decidan ir a lo grande, y busquen en algún lugar que contenga mucha información, por ejemplo, algún sitio web de ventas en línea. Las bases de datos de sitios de ventas en línea poseen una gran cantidad de información de una variedad de usuarios. Ya que hasta un 70% de las transacciones se pueden llevar a cabo con tarjetas de crédito, estos lugares pueden tratar de ser atacados.

¿Cómo podemos protegernos?

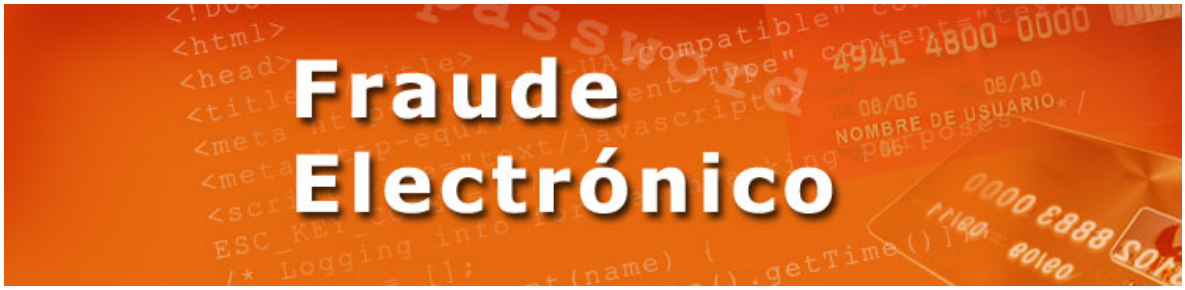
Las acciones preventivas son nuestra mejor arma a la hora de pelear contra estos maleantes de Internet. Es importante que tomemos responsabilidad acerca de nuestras actividades comerciales y financieras en línea, tal y como lo hacemos cuando entramos a una tienda o vamos al banco.

Además de las más comunes (memorizar nombres de usuario y contraseñas, no compartir estos datos con nadie, utilizar solo sitios seguros, etc.), existen algunas otras recomendaciones que podrían sernos de utilidad como se puede ver en la sección de *Tips* en este número.

Ya me pasó, ¿qué hago?

En caso de que nos encontremos ya en una situación de fraude electrónico es importante reportarlo lo más pronto posible a nuestra institución bancaria. La prontitud en nuestras acciones puede, en la mayoría de los casos, ser la diferencia para detener el problema y, posiblemente,

[1]Generador de números para reconocer identidad



capturar a los malhechores. Además, algunos bancos exigen prontitud para responder por los reclamos. Bancomer, por ejemplo, no acepta reclamos realizados más de dos días después del incidente.

En todo caso, es importante tener todos los datos del incidente, para poder realizar un reporte apropiado. Fechas, montos y tipo de movimientos son importantes indicadores, así como, por supuesto, los números de cuenta involucrados. Siempre se nos exigirá presentar documentación oficial que nos acredite como los titulares de la cuenta afectada, aunque los documentos solicitados varían según el caso.

Dentro de los problemas que se deben reportar se encuentran:

- Posibles accesos no autorizados a nuestra cuenta.
- Movimientos irregulares.
- Cargos no autorizados.
- Pérdida de contraseña.
- Pérdida de *token*.

Sin embargo, es necesario tener presente que la mejor manera de combatir este tipo de problemas es prevenirlos.

[1]http://amipci.org.mx/estudios/temp/estudio_amipci_2006_version_web-07888300011636083260B.pdf
http://amipci.org.mx/estudios/temp/Estudio_AMIPCI_comercio_electronico_2008_pdf-08245730012203807810B.pdf

Pescando Información: *Phishing*

Miriam J. Padilla Espinosa

El avance de la tecnología no sólo ha influido en facilitar las actividades cotidianas, sino también en su uso para actos delictivos y se aprovechan de la falta de información e ingenuidad de los usuarios, tal es el caso de la actividad conocida como ***phishing***. La cual ha generado pérdidas económicas tanto al sector empresarial como a los particulares durante los últimos años.

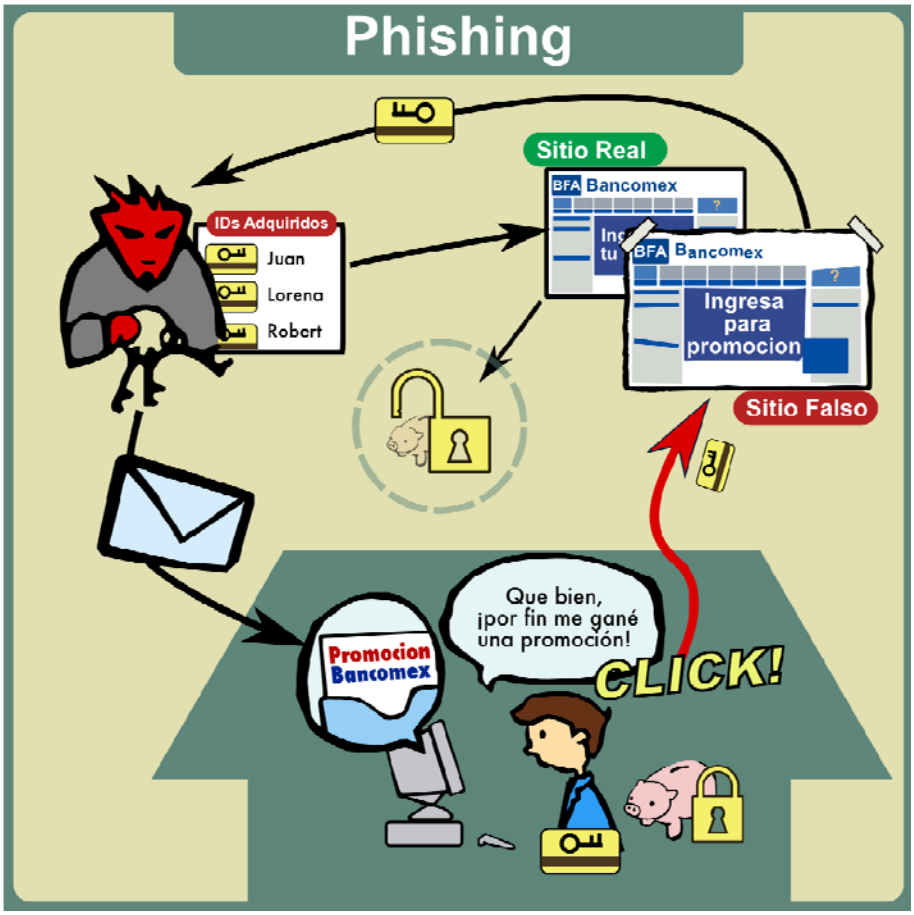


Ilustración: Iván Santa María

El *Phishing* consiste en el envío de mensajes (anzuelos) a una o varias personas, recurriendo a la suplantación de identidad de una empresa o entidad pública con el objetivo de persuadir a la futura víctima para revelar sus datos personales o financieros que involucran nombres de usuario y contraseñas. Una vez obtenida esta información es utilizada con fines maliciosos como transferencias de fondos a cuentas bancarias y compras con tarjetas de crédito entre otras acciones delictivas que afectan económicamente a la víctima.

En la actualidad la actividad de *phishing* utiliza principalmente el correo electrónico enviando correos falsos por parte del atacante. En estos correos se solicitan contraseñas o detalles de las cuentas bancarias argumentando comúnmente situaciones como problemas técnicos, procesos de actualización y revisión de datos buscando aprovecharse de la ingenuidad de los usuarios para obtener información. En algunos casos se emplean técnicas más sofisticadas como el uso de sitios web falsos, instalación de caballos de Troya[2], *key-loggers*[3], *screen-loggers*[4], envíos de mensajes de SMS, mensajes en contestadores automáticos y llamadas telefónicas.

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

Los tipos de *phishing* se pueden clasificar considerando las técnicas mediante las cuales se lleva a cabo la obtención de la información, estos tipos se ilustran en la Tabla 1. Preocupado por disminuir esta actividad delictiva el Departamento de Seguridad en Cómputo (DSC) de la DGSCA, a través de su equipo de respuesta a incidentes, pone a disposición del público la dirección electrónica ***phishing@seguridad.unam.mx*** para el reporte de incidentes de tipo *phishing*. Esto contribuye a reducir esta actividad delictiva y los impactos a nivel económico que ocasiona. Mediante el estudio de los casos que han sido reportados al DSC/UNAM-CERT se obtiene el Gráfico 1:

[2] Programa malicioso que aparenta ser benigno. Es utilizado para obtener el acceso a un sistema para comprometerlo.
[3] Herramienta que detecta las pulsaciones que se realizan en el teclado.
[4] Herramienta que capturan las imágenes de las pantallas.

Pescando Información: *Phishing*

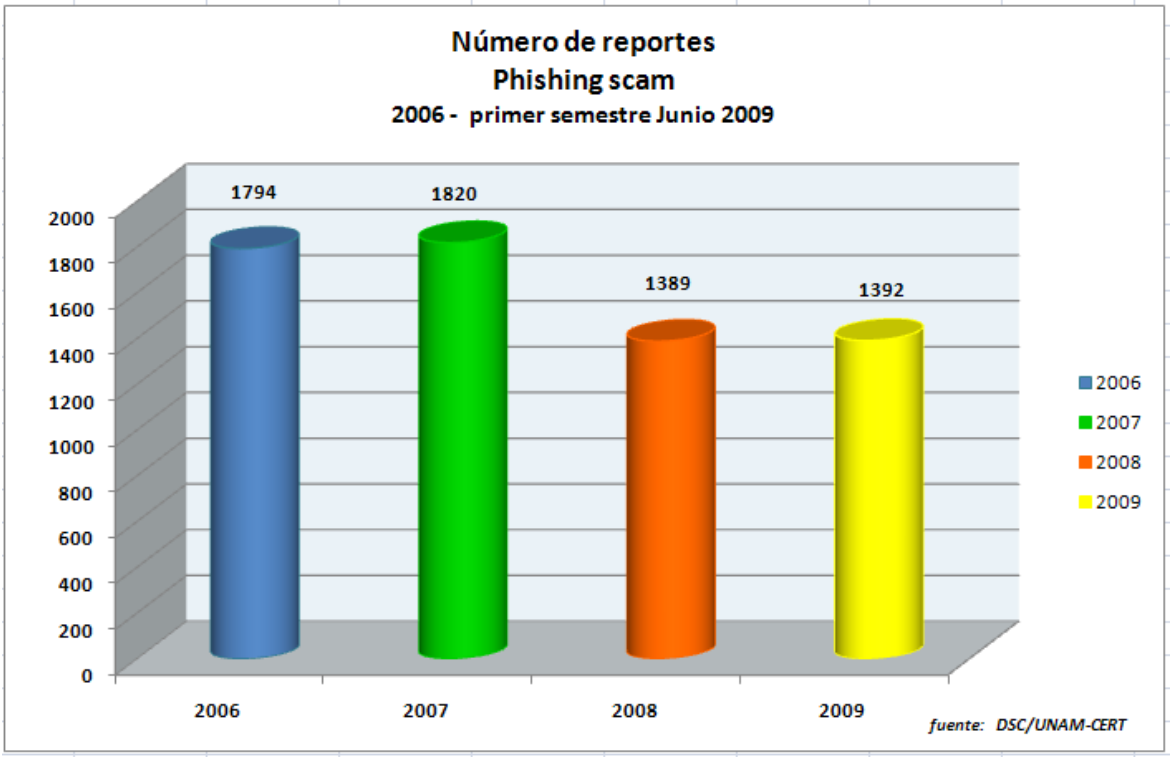


Gráfico 1.

Se muestra el comportamiento que ha tenido la actividad de *phishing* en el periodo de 2006, hasta el primer semestre del 2009. Se puede ver que en el último semestre se han registrado un número mayor de casos que los reportados en todo el año 2008 lo cual representa una alerta importante para que los usuarios consideren medidas preventivas que eviten que su información personal y financiera sea robada y utilizada con fines delictivos. En la mayoría de los casos esta actividad está orientada a obtener acceso a información financiera, pero de igual forma es utilizada para apoderarse de cuentas de correo público, lo que conlleva a una pérdida considerable de información ya que sus cuentas pueden ser comprometidas para otro tipo de ilícitos.

La forma en la cual los usuarios pueden evitar ser una víctima es mediante mecanismos de prevención y protección. En la Tabla 2 se muestra una serie de recomendaciones para NO ser víctimas de *phishing*.

RECOMENDACIONES PARA EVITAR SER VÍCTIMA DE PHISHING	
• Sospechar ante cualquier correo electrónico que solicite información personal mediante argumentos como, problemas técnicos, promociones de nuevos productos o servicios, premios o actualización de datos.	
• Nunca proporcionar información como nombres de usuario, contraseñas, número de tarjetas de crédito o fechas de caducidad, vía telefónica ni vía correo electrónico bajo ninguna circunstancia.	
• Los mensajes de correo electrónico de phishing frecuentemente carecen del nombre y apellido completo del usuario, por el contrario, los correos legítimos enviados por las instituciones financieras siempre incluyen el nombre completo.	
• Los usuarios no deben rellenar información personal o financiera en formularios de correos electrónicos.	
• No utilizar los enlaces incluidos en correos electrónicos de dudosa procedencia, para ello es recomendable dirigirse a la página web de la entidad o la empresa de forma directa.	
• Antes de proporcionar cualquier dato sensible como datos bancarios, números de tarjetas de crédito, contraseñas asegúrese de que se encuentra en una web segura.	
• Que siempre el navegador web, esté actualizado y que cuente con los últimos parches de seguridad instalados.	
• A continuación se listan los principales proveedores de barras antiphishing:	
Netcraft *http://toolbar.netcraft.com/* ***Filtro de Suplantación de Identidad (Phishing) en Microsoft Internet Explorer 7*** *http://www.microsoft.com/danmark/windows/ie/default.mspx#ie7security* ***Cloudmark Anti-Fraud Toolbar*** *http://www.cloudmark.com/desktop/ie/*	***Filtro de Phishing en Firefox 2.0*** *http://www.mozilla.com/en-US/firefox/phishing-protection/* ***EarthLink Scamblocker*** *http://www.earthlink.net/software/free/toolbar/* ***Microsoft Phishing Filter Add-in for MSN Search Toolbar*** *http://addins.msn.com/phishingfilter/*

Tabla 2

Referencias:

http://seguridad.internautas.org/html/451.html
http://www.microsoft.com/spain/empresas/legal/phishing.mspx
http://www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx
http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/
http://www.segu-info.com.ar/malware/phishing.htm
http://megustaelturismo.es/blog/2008/03/13/explicacion-de-los-distintos-tipos-de-phishing/
http://www.arcert.gov.ar/webs/tips/recomendaciones_phishing.pdf
http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf
http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf
http://www.seguridad.unam.mx/usuario-casero/secciones/phishing.dsc#barras
http://www.cert.org.mx/estadisticas.dsc

Juan Patiño Corona

Las nuevas tecnologías ofrecen un alto nivel de comodidad y eficiencia lo que ha fomentado enormemente el uso de las mismas. Pagar las cuentas, realizar transferencias bancarias, consultar nuestro estado financiero, inclusive pedir una pizza o rentar un DVD, etc. Son sólo unas pocas de las tantas actividades que podemos hacer en Internet, la parte delicada es cuando para hacer uso de estos servicios debemos compartir información personal o privada.

Es aquí donde podríamos preguntarnos: ¿Cómo no dar mi dirección a una tienda si quiero que me envíen un paquete? o ¿Cómo pedirle a mi banco que transfiera el dinero de mi cuenta a otra sin proporcionarle una serie de datos confidenciales? Por supuesto que no siempre podemos exigir información sin antes compartir un poco, al final de todo, nuestra contraparte debe de estar segura que somos quienes decimos ser. ¿Pero nosotros estamos seguros de que ellos son quienes dicen ser? Aquí es donde comienza este ataque llamado *pharming* y la muy estrecha relación que guarda con el *phishing*.

Objetivos del *pharming*

El fraude hoy en día es uno de los crímenes que encabezan la lista de delitos informáticos en nuestro país y los objetivos del *pharming* en su mayoría se dirigen a obtener beneficios económicos e información privilegiada, muchas veces para la generación de estafas.
Este tipo de ataque generalmente busca la obtención de:

- Información bancaria.
- Credenciales de acceso (nombre de usuarios y contraseñas).
- Información personal (números telefónicos, direcciones, e-mail, etc).

Es importante recalcar que en la mayoría de los casos el *pharming* se dirige a la creación de fraudes, pero tiene un campo de acción mayor, por ejemplo puede emplearse para dirigir a los clientes de un DNS comprometido a páginas web donde se les descargará código malicioso forzando la generación visitas en algún sitio cuando los clientes tecleen la dirección de algún portal conocido, valiéndose de su popularidad. En fin, los objetivos pueden ser muchos y tan variados como los deseos que tenga el atacante.

¿Qué es el *pharming*?

Cuando ingresamos la dirección de una página de Internet por ejemplo www.seguridad.unam.mx esta dirección debe traducirse a su correspondiente numérico denominado dirección IP, compuesta de cuatro grupos de números que tienen un rango definido entre el 0 y el 255. Por ejemplo para el caso del portal www.seguridad.unam.mx corresponde la dirección IP 132.248.124.130.

Esta traducción es tarea del Servidor de Nombres de Dominio (DNS por sus siglas en ingles) y en ocasiones puede ser realizada a través de archivos localizados en nuestras computadoras o tablas configuradas en nuestros *routers*.

Conociendo lo anterior, podemos comenzar a decir que el *pharming* es un ataque informático donde se manipulan estos registros, usualmente a través de la ejecución de algún código malicioso, por lo regular en forma de troyano.

Imaginemos que estamos frente a una computadora víctima de este *malware* capaz de modificar la información de los DNS e ingresamos la URL de una página bien conocida, pero sin saberlo estamos siendo direccionados a otro lugar que al igual que el *phishing*, aquí podremos ser testigos de una suplantación de identidad, un engaño y un peligroso fraude informático.

Una forma más sencilla de explicar y entender el *pharming* puede ser mediante un ejemplo: suponga que un día como cualquier otro que se dispone a pagar una cuenta, usted teclea la dirección URL de su banco, y es direccionado a un sitio con una apariencia idéntica, pero en realidad es la página que un usurpador ha clonado para obtener su información

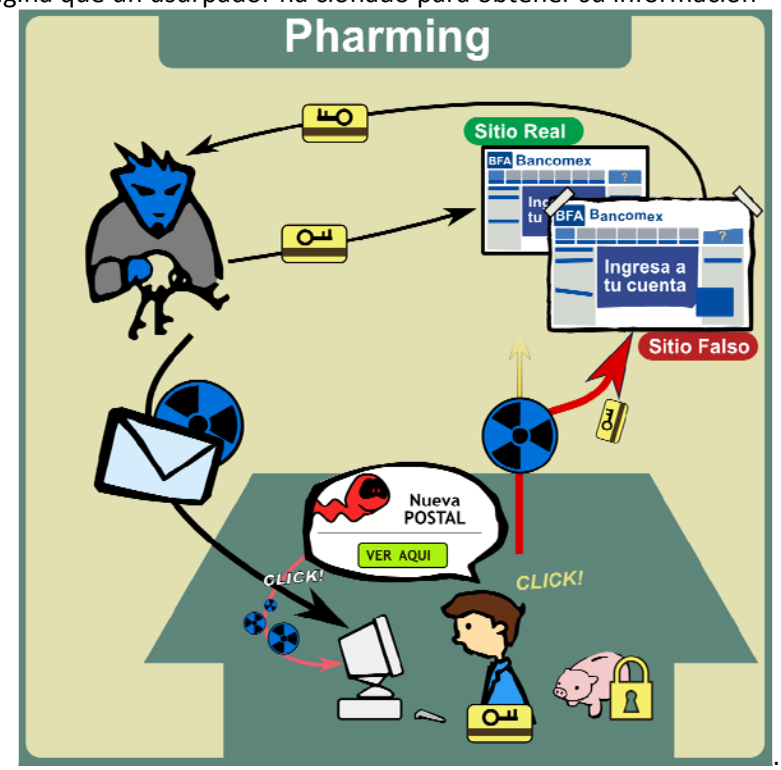


Ilustración: Iván Santa María.

Ahora completamente confiado de que la dirección que usted tecleó es la auténtica transfiere dinero de su cuenta a otra, en este momento el atacante tendrá lo necesario para realizar la misma acción sin la necesidad de su autorización, fácilmente puede ejecutar el mismo proceso de transferencia pero probablemente el destino de ese dinero sea la cuenta del mismo estafador.

Resulta importante recalcar que el punto medular de la peligrosidad de éste ataque radica en el hecho de que pasa prácticamente inadvertido por las víctimas, a través del proceso de traducción

de la dirección URL a la dirección IP, haciendo que el usuario que conscientemente intenta ingresar a una página web legítima, esté siendo direccionado a otra parte sin enterarse.

Diferencia entre *pharming* y *phishing*

Hasta este punto parece que estamos hablando de *pharming* como sinónimo de *phishing*, pero hay una diferencia radical. El *pharming* va mas allá ya que puede afectar a maquinas de manera individual o a redes enteras que hagan uso del mismo servidor DNS o dispositivo comprometido, lo que permite que el atacante tenga bajo su control a un grupo de usuarios vulnerables tan grande como la cantidad de clientes del Servidor DNS contaminado lo que resulta más peligroso, pues mientras el *phising* requiere que cada usuario acceda al link del estafador para convertirse en una potencial víctima, el *pharming* sólo necesita que alguien haga una consulta legítima al servidor DNS modificado, haciendo que muchas precauciones tomadas para protegerse del *phishing* no sean suficientes ni útiles para evitar el *pharming*.

Consejos de prevención del ataque

- No abrir o leer correos electrónicos de los cuales no confirmemos su procedencia y legitimidad.
- Verificar que los portales que visitamos emplean un protocolo seguro como https en lugar de http, así mismo cerciorarse que el certificado de seguridad sea válido.
- Revisar frecuentemente el archivo *hosts*. Este archivo contiene registros de traducción de nombre de dominio a dirección IP y se localiza en “C:\Windows\System32\drivers\etc\hosts” para sistemas Microsoft Windows o en “/etc/hosts” para sistemas basados en UNIX. Con el fin de identificar y borrar los registros desconocidos, de la misma manera se recomienda analizar las tablas de traducción de nuestro *router* si éste cuenta con esa opción.
- No emplear permisos de administrador para tareas cotidianas que no requieran dicho privilegio, esto evitará que algún código malicioso pueda modificar el archivo *hosts* o cualquier otro archivo del sistema.
- Denunciar cualquier incidente de este tipo a la dirección phishing@seguridad.unam.mx

Referencias:

http://www.seguridad.unam.mx/usuario-casero/secciones/pharming.dsc
http://blogs.eset-la.com/laboratorio/2007/08/10/troyanos-haciendo-pharming-local-bancos/
http://www.microsoft.com/spain/empresas/legal/pharming.mspx

¿Intermedios para Transferencias Monetarias?

Rocío del Pilar Soto Astorga

El realizar tus compras por Internet puede llevarse a cabo de la manera estándar en la que realizas un depósito bancario o mediante tarjeta de crédito directamente en la página de la compra, sin embargo existe la posibilidad de hacer uso de los conocidos como “Servicios de pago a terceros”.Estas empresas sirven de intermediario brindando varios servicios como son la transferencia de dinero entre cuentas, compras en línea, pago en subastas y donaciones altruistas. Algunas de ellas incluso pueden funcionar para el simple envío de dinero de persona a persona. Con ello evitas revelar el número de tu tarjeta de crédito o parte de tu información bancaria en cualquier página de Internet.

Supongamos como ejemplo que un usuario entra a Internet y quiere comprar un libro que vio en una página, un apuntador láser que vio en otra, necesita hacer una transferencia de dinero y de casualidad encuentra un anhelado modelo a escala de un F-14 en una subasta. Para hacer los pagos correspondientes cuenta con su tarjeta de crédito e ingresa sus datos en cada uno de los sitios que ve. La información de su tarjeta se encuentra ahora en varios sitios de una red mundial y esto no es deseable para la mayoría de nosotros (además de que existe el riesgo de caer en un sitio falso).

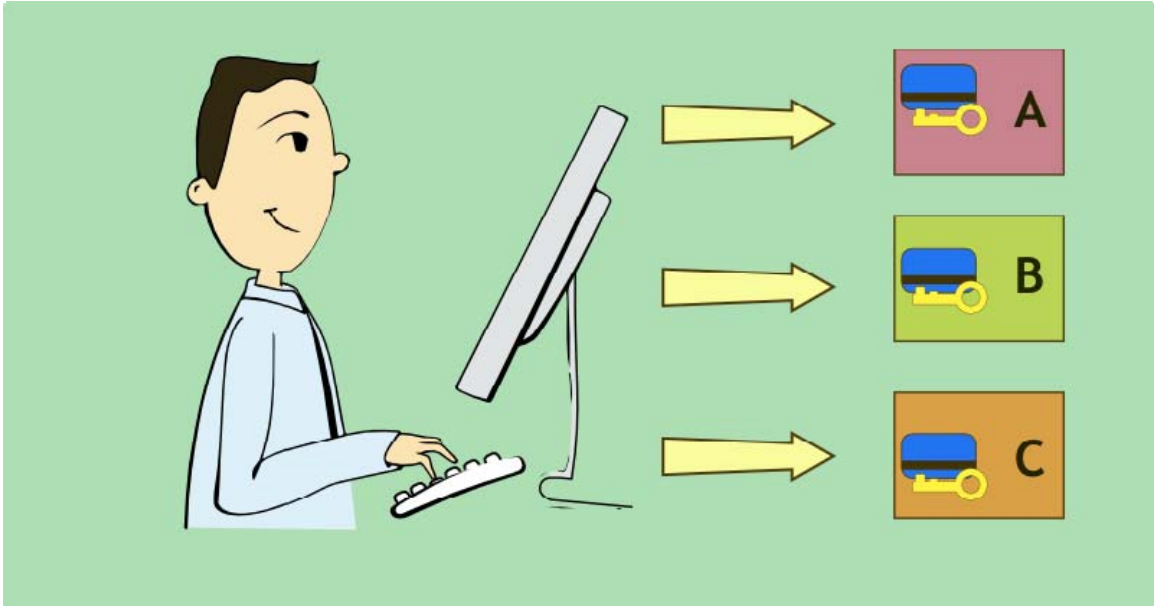


Ilustración: Iván Santa María

Por otra parte, si el usuario abre una cuenta en un servicio intermediario de pago, se realiza la transferencia de su tarjeta de crédito a la cuenta en este servicio. El pago a los diferentes sitios de compra, subasta y transferencia se realizarán a desde la cuenta en el servicio intermediario por lo que su información bancaria ya no es distribuida.

¿Intermedios para Transferencias Monetarias?

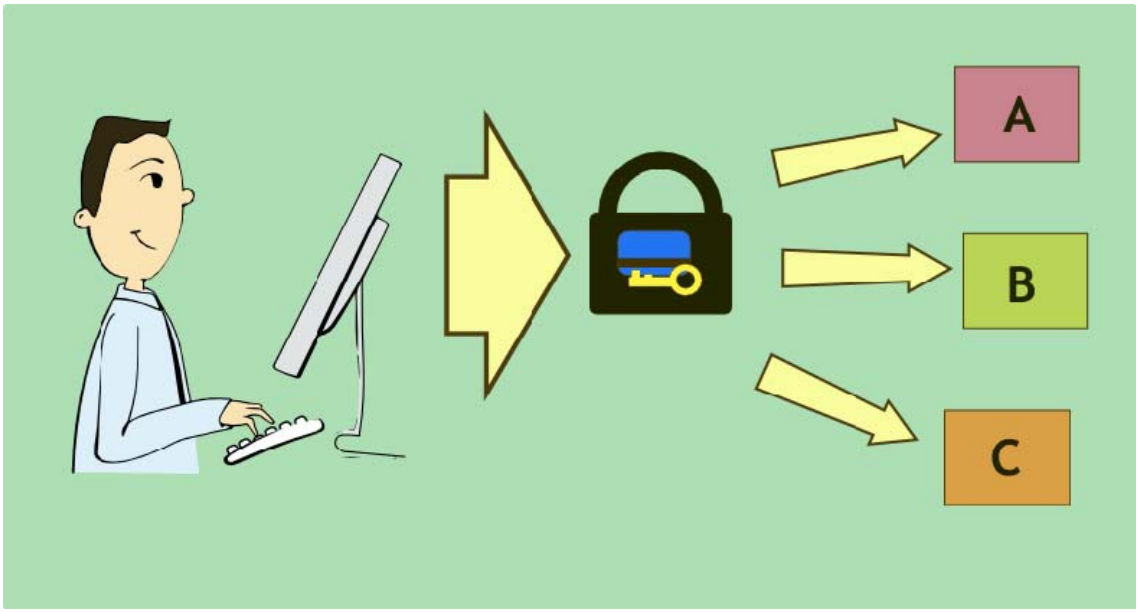


Ilustración: Iván Santa María

Entre los sitios en Internet que ofrecen estos servicios se encuentran PayPal, Amazon *Payments*, Google *Checkout*, *moneybookers* entre otros muchos.

La forma en que operan estas empresas es, por lo general, creando una cuenta dentro de ellas por medio de la cual se realizarán los pagos y transacciones sin tener que revelar tu información bancaria. La empresa intermediaria realiza el cobro al comprador mediante un cargo a su tarjeta de crédito o por medio de otro tipo de pago que sea permitido en el contrato.

Hay que tomar varios puntos en cuenta al momento de elegir uno de estos servicios, entre estos puntos se encuentran:

- Los sitios en los cuales esta empresa puede servir de intermediario. Algunas páginas de Internet solo aceptan ciertos intermediarios porque como vendedores pagan a estos intermediarios por un servicio.
- Revisar que los servicios que ofrece satisfacen enteramente nuestras necesidades. Es decir si cuentan con todo aquello que solemos emplear: pago en subastas, compras en línea, transacciones bancarias…
- Ver las tarifas que se tienen para cada servicio. Algunos de estos sitios solo le cobran al vendedor siendo gratuito para aquel que compra, sin embargo no es una regla general.
- Como se maneja los tipos de cambio. Gracias a que Internet nos conecta a distintas partes del mundo, nos encontraremos con algún movimiento de dinero que requiera el cambio de divisa por lo que debemos estar enterados en cómo se lleva a cabo este tipo de cambio.
- Conocer el monto máximo que puede ser manejado en una transacción.
- Informarse sobre si la cuenta creada con la empresa cuenta con algún tipo de seguro.

- Revisar las políticas de seguridad y políticas de reembolso.

Además de estas recomendaciones para la elección de la empresa que sirva de intermediario se deben tomar en cuenta también precauciones en cuanto a caer en engaños como el *Phishing* y *Pharming* tratados también en este número.

Referencias:

http://www.microsoft.com/latam/athome/security/privacy/onlinepayments.mspx
http://help.yahoo.com/l/e1/yahoo/paydirect/faq/faq-06.html
http://www.paypal.es/es
http://www.auctionbytes.com/cab/abu/y202/m11/abu0083/s02
http://checkout.google.com

Carmina Cecilia Espinosa Madrigal
Miriam Valdés Rodríguez

Antes de realizar una compra o transacción en línea es importante saber *dónde*, *cómo*, *a quién* y *bajo qué condiciones* se va a llevar a cabo. Por tal motivo te presentamos algunos elementos básicos que te permitan reconocer páginas o sitios que ofrecen servicios de comercio electrónico de manera segura y confiable.

Existen elementos que puedes identificar en tu navegador al consultar un sitio Web para comprobar que la información que estas compartiendo se transfiere de forma segura, es decir, que garantice que un usuario externo no pueda tener acceso a ella. Estos elementos se mencionan a continuación.

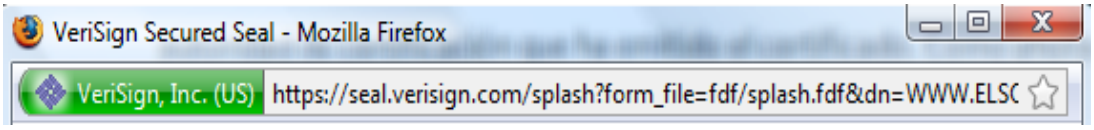
Símbolo del candado de seguridad

El candado de seguridad indica que el sitio utiliza el Protocolo de Capa de Conexión Segura SSL por sus siglas en inglés. Este protocolo permite establecer una comunicación cifrada entre tu navegador y el servidor de un sitio Web, de esta manera se realiza la transferencia de información confidencial de forma segura.

Tips para Evitar Fraudes en Línea

Transacciones protegidas e identidad del sitio web

Los sitios Web de alta seguridad muestran una barra de direcciones con el nombre del sitio web autenticado y el nombre de la autoridad certificadora que ha emitido el certificado.



Sellos de confianza

- El sello de la firma de seguridad *VeriSign* indica que compañía le otorgó un certificado de identidad que lo avala bajo estándares específicos de seguridad Estos certificados son reconocidos por todos los navegadores Web como confiables.
- Para sitios de Internet en México puede aparecer el sello de confianza AMIPCI® otorgado por la Asociación Mexicana de Internet (AMIPCI), este reconoce a los negocios o instituciones que promueven el cumplimiento de la privacidad de la información y están legítimamente establecidos.

Cookies

Una *cookie* es un dato creado por un servidor Web el cual se almacena en la computadora del usuario.

Éstas contienen información personal (nombres de usuario y contraseñas) que pueden ser objeto de ataques de código malicioso. Una recomendación para incrementar la seguridad en línea es borrar periódicamente las *cookies*. Para ello, los navegadores ofrecen la opción de limpiar datos privados.

Otra medida preventiva es instalar software de seguridad en tu computadora como los antivirus que ayudan a disminuir el riesgo de que tu información personal se vea comprometida.

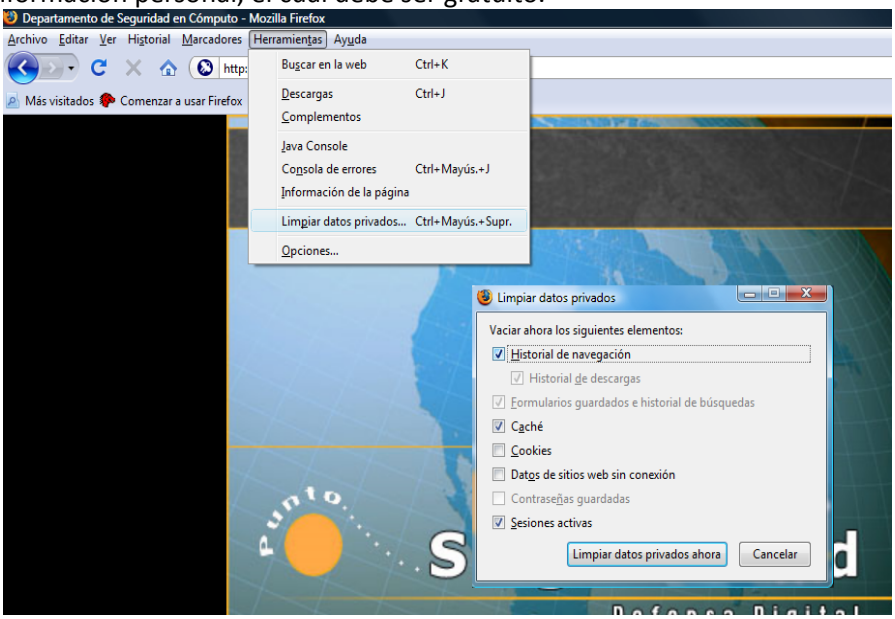
Y recuerda que antes de hacer una compra en línea...

1. Verifica la existencia del sitio que te ofrece el servicio. Esto lo puedes hacer con la información de contacto que se proporciona en el mismo, tal como correo electrónico,

teléfono, fax y domicilio.

2. Lee las políticas de privacidad, en ellas el sitio te da a conocer cómo, para qué y quiénes van a tener acceso a la información que proporciones; así mismo revisa el contenido de las políticas de cancelación, devolución y reembolso de productos o servicios.

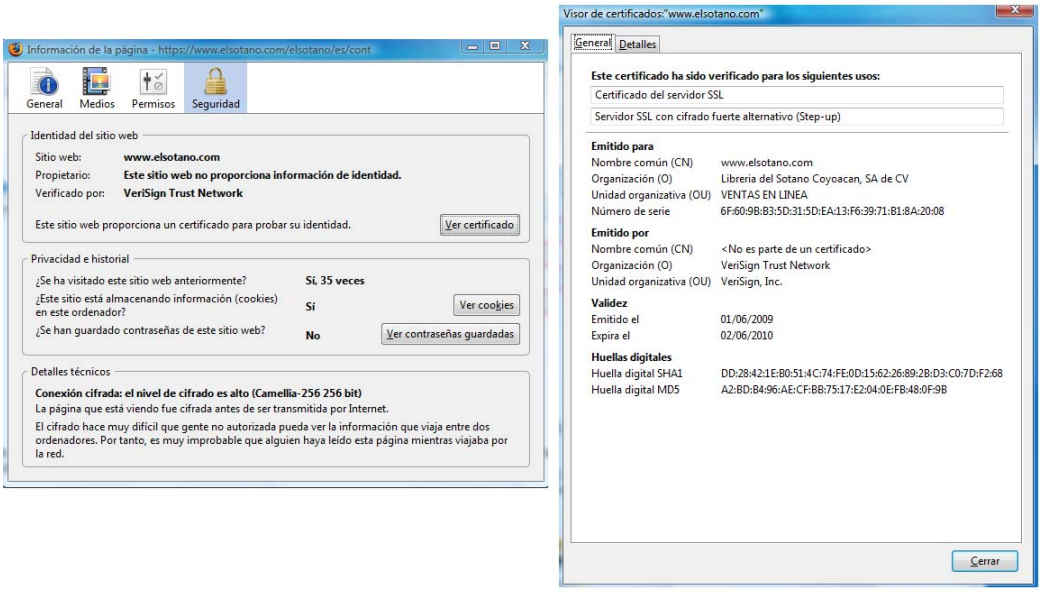
3. En todos los sitios de comercio electrónico por Internet, es necesario llenar un registro con información personal, el cual debe ser gratuito.



4. Verifica que el sitio en donde vas a realizar el registro cuenta con los siguientes elementos de seguridad:

a) En tu navegador, la dirección de la página debe comenzar con **https**, lo que indica que es un sitio seguro. Sin ningún tipo de advertencia sobre la validez del certificado.

b) En la barra de estado (parte inferior de la ventana del navegador) debe aparecer la imagen de un candado cerrado o una llave.
c) Sobre el candado de seguridad haz doble click y aparecerá el certificado de seguridad, el cual debe estar vigente.



5. Si estas realizando una compra, confirma que tu orden tenga exactamente lo que seleccionaste, de no ser así, corrige tu orden antes de enviarla.

6. No compres en sitios que se promuevan en correo electrónico no deseado o *spam*.

7. Al momento de realizar tus pagos procura utilizar cheques, depósitos en la cuenta bancaria del vendedor o servicios de pago en línea intermedios (como *Paypal*, Google *Checkout*, entre otros) ya que de esta manera podrás comprobar las transacciones realizadas.

8. Para cualquier duda o reclamación, conserva el número de identificación de la compra y tus comprobantes de pago.

9. Evita hacer uso del comercio electrónico en los café Internet ya que existe una alta probabilidad de que se haya instalado un software dedicado al robo de información personal.

Recuerda que los sitios de comercio electrónico confiables ofrecen todos los elementos para que tu compra sea segura evitando que tengas una mala experiencia.

Referencias:

https://www.verisign.com/ssl/secured-seal/index.html
http://www.profeco.gob.mx/encuesta/brujula/bruj_2007/bol34_comp_red.asp
http://www.econsumer.gov/espanol/
http://www.profeco.gob.mx/encuesta/brujula/bruj_2005/b03_comsegura.asp
http://www.sellosdeconfianza.org.mx/quesello.php
https://www.paypal.com/mx/cgi-bin/helpscr?cmd=_products-services-outside&nav=3
http://www.verisign.es/ssl/ssl-information-center/ssl-resources/index.html
http://www.verisign.es/ssl/ssl-information-center/ecommerce-trust-ssl/index.html
http://www.ecommercetimes.com/story/33567.html?wlc=1245292844
http://www.elsotano.com/

Seguridad TV

Jesús Mauricio Andrade Guzmán

El sitio Web de Seguridad TV es un esfuerzo del Departamento de Seguridad en Cómputo por establecer contacto con los usuarios que no cuentan con conocimientos técnicos de seguridad informática para tener una experiencia más informada y segura al navegar en Internet.

¿A qué usuarios está dirigido?

En pocas palabras, a cualquier usuario. El contenido que se ofrece en este sitio ha sido pensado para cualquier persona interesada en la seguridad en cómputo de cualquier edad o especialidad. El sitio cuenta con un listado de programas con lo que podrás encontrar de manera sencilla cualquier programa que se haya transmitido o esté programado para un día en específico.

¿Qué secciones ofrece el sitio?

Puedes encontrar manuales en video, explicaciones sencillas para conceptos de seguridad y noticias en el campo de la seguridad en cómputo sobre amenazas que puedes encontrar al navegar en Internet. También puedes encontrar programación especial para presentar temas relevantes en el campo de la seguridad en cómputo. El sitio permite navegar entre contenidos especializados como: códigos maliciosos, pruebas realizadas con herramientas en monitoreo de redes, *honeynet*, difusión de sitios sospechosos de *phishing* y *pharming*, técnicas para reconocer correos no deseados (SPAM), manuales de instalación y configuración de seguridad para servicios de red (Web, correo, bases de datos, etc.)

¿Qué servicios ofrece?

Puedes suscribirte para recibir información sobre nueva programación y documentos relacionados con los programas para complementar los temas que se presentan. Esta información y mucho más está a tu alcance al acceder a la siguiente dirección:

http://tv.seguridad.unam.mx

DIRECTORIO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dr. José Narro Robles
Rector

Dr. Sergio Alcocer Martínez de Castros
Secretario General

DIRECCIÓN GENERAL DE SERVICIOS DE
CÓMPUTO ACADÉMICO

Dr. Ignacio de Jesús Ania Briseño
Director

Ma. de Lourdes Velázquez Pastrana
Directora de Telecominicaciones

Ing. Rubén Aquino Luna
Responsable del Departamento de Seguridad en Cómputo UNAM-CERT

Revista elaborada por la
Dirección General de Servicios de Cómputo Académico

CRÉDITOS

PUNTO SEGURIDAD, DEFENSA DIGITAL

M en I. Rocío del Pilar Soto Astorga
Edición

Jesús Mauricio Andrade Guzman
Sergio Andrés Becerril López
Carmina Cecilia Espinosa Madrigal
Miriam J. Padilla Espinosa
Juan Patiño Corona
Javier Ulises Santillán Arenas
Rocío del Pilar Soto Astorga
Miriam Valdés Rodríguez
Iván Santa María González
Colaboraciones

Ing. Rubén Aquino Luna
Responsable del Departamento de Seguridad en Cómputo UNAM-CERT

Roberto Sánchez Soledad
Coordinador de Contenidos

Act. Guillermo Chávez Sánchez
Coordinación de Edición Digital

Lic. Lizbeth Luna González
Dolores Montiel García
L.D.C.V. Carolina Silva Bretón
Diseño Gráfico

Diana Chávez González
Liliana Minerva Mendoza Castillo
Formación

2009 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico