La SEGURIDAD en el mundo digital

Guillermo M. Mallén Fullerton

La pérdida de privacidad y el espionaje son sin duda los problemas de seguridad más serios que tenemos en Internet, debido a su volumen y universalidad. En este artículo se analizan éstos y otros aspectos, y se sugieren medidas y hábitos que pueden garantizar la confidencialidad de información de carácter privado.

Privacidad: el amor en los tiempos de Facebook

Por fin, Alejandro decidió sentar cabeza y dejar de andar correteando chicas. Por fin encontró a quien será el amor de su vida. Por tres meses todo ha ido muy bien: la relación es seria y tiene la apariencia de ser para siempre. Sin embargo, algo raro ocurre: su gran amor ha dejado de hablarle intempestivamente. Él hace un esfuerzo y logra contactar a su novia, quien lo acusa de mujeriego y poco serio.

¿Qué ocurrió? Resulta que Alejandro abrió, hace unos tres años, una cuenta en Facebook e invitó como amigos a todos los que estaban en su libreta de direcciones de correo electrónico, algo completamente normal. Rápidamente perdió el interés y abandonó la cuenta. Sólo que la cuenta no se borró, y los amigos que invitó inicialmente suben muchas fotos de vacaciones, fiestas, borracheras y demás, y les ponen las etiquetas o *tags* que identifican a cada una de las personas que aparecen en ellas.

Cuando cualquier amigo de Alejandro entra al Facebook de él, aparecen enormes colecciones de fotos tomadas por todos sus contactos y en las que él aparece. En muchas de las fotografías está en poses comprometedoras con alguna chica. Ver la sucesión de fotos es ver la historia de las muchas conquistas de Alejandro.

La novia de Alejandro también está en Facebook –¿quién no, hoy en día?– y se le ocurrió buscar la cuenta de su novio. Mandó la invitación para ser "amigos",

pero pasó un tiempo y no recibió respuesta. Vio entonces que entre los amigos de Alejandro estaba una gran amiga de ella, quien le dio acceso a las fotos de él y ¡oh sorpresa!, al verlas vio también la historia de conquistas de su novio y decidió cortar por lo sano.

Casos como éste se repiten a diario, no sólo en las relaciones amorosas, sino de otro tipo, que también suelen traer consecuencias no deseadas bastante importantes, como en el medio laboral, donde las redes sociales se usan cotidianamente para investigar a los candidatos a los diferentes puestos vacantes en empresas y gobiernos, y que en muchas ocasiones niegan, sea correcto o no, el empleo a las personas al ver comentarios o fotografías que indican algún elemento no deseado, como las ideas políticas de las personas o un estilo de vida cuestionable para algunos.

Esta tendencia ha llegado a tal grado que algunos gobiernos han intentado prohibir a los empleadores usar las redes sociales como fuente de información sobre los candidatos a contratar. Sin embargo, cuando a alguien le dicen "es usted un buen candidato, pero en esta ocasión encontramos a alguien mejor, así que lo consideraremos para la próxima vez", ¿cómo puede saber si en verdad a quien contratan es mejor, o si simplemente encontraron algo que no les gustó en alguna de las redes sociales?

La información que ponemos en las redes sociales no es la única que hay sobre nosotros en Internet. En muchas ocasiones colocamos comentarios en *blogs* o votamos por alguna canción o película. Esta información, junto con nuestra clave de usuario y otros datos personales, quedan almacenados en los servidores de la red, y puede ser utilizada con posterioridad por el dueño del servicio. En muchos casos hay políticas de privacidad que proporciona el propio dueño del servicio para protegernos y para que tengamos más libertad al expresar nuestros comentarios o preferencias; sin embargo, es importante siempre leer esas políticas, pues con demasiada frecuencia ofrecen poca protección a nuestra privacidad, y en el fondo son más bien una autorización para que el dueño del sitio haga lo que quiera con nuestros datos.

En México tenemos una ley de protección de datos privados que entra en vigor en 2011, pero aunque está bastante bien hecha y proporcione buenas herramientas para que los usuarios eliminen datos y limiten el uso de los mismos, la inmensa mayoría de los sitios de Internet no están en México, y no tienen por qué sujetarse a nuestras leyes.

Netflix y las preferencias personales

En apariencia, expresar un comentario en Internet o votar por un artista o una canción no tiene nada de particular. Finalmente nosotros sabemos lo que pusimos y estamos protegidos por la política de privacidad del sitio de Internet, ¿o no?

Hace poco tiempo, en 2009, hubo un incidente que expuso mucha información sobre las preferencias de los usuarios. En Estados Unidos existe un servicio de renta de películas denominado Netflix (*www.netflix.com*). A fin de dar un buen servicio, esta empresa pide a sus clientes que califiquen cada película que han alquilado, de manera que se les pueda sugerir más películas que coincidan con sus gustos. Esto no es nuevo; desde hace buen tiempo lo hacen sitios como Amazon y realmente resulta cómodo para los clientes.

Con el fin de mejorar la calidad del servicio, Netflix ofreció un millón de dólares a quien mejorara el modelo de predicción de preferencias en el que se basan las recomendaciones. Para ello, liberó una base de datos bastante grande con la información sobre preferencias proporcionados por sus clientes. De acuerdo

con su política de privacidad, anonimizaron la base de datos dando simplemente un número a cada cliente.

El concurso (*www.netflixprize.com*) se llevó a cabo, y logró una mejoría interesante en la calidad de las predicciones. Pero dos investigadores de la Universidad de Texas en Austin lograron ligar, con todo rigor científico (*www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf*), a los usuarios de Netflix con los de la base de datos Internet Movie Database (*www.imdb.com*), en la que se califican películas de forma pública, no anónima. De esta manera, la anonimidad ofrecida por Netflix se perdió, y salió a flote información que debería haber permanecido confidencial. Así por ejemplo, los autores del artículo obtienen, entre otras cosas, las preferencias políticas de las personas, información que seguramente muchos de los usuarios de Netflix quisieran mantener privada, pero que seguramente es codiciada por los partidos políticos y el gobierno de Estados Unidos.

Podríamos calificar lo ocurrido a Netflix como un accidente debido a una manera ingenua de anonimizar los datos. Sin embargo, hay otros casos en los que la obtención y uso de la información son deliberados.

Amazon.com y los hábitos de compra

Consideremos el caso de las tiendas *online* como Amazon. Registran no sólo la historia de las compras que hemos realizado, sino también las *wishlist* (listas de deseos) y todos los artículos que hemos visto, aunque no los hayamos comprado. Con base en esta información, seleccionan los artículos que nos sugieren. Pero hacen algo más: nos clasifican junto con otros usuarios que tengan perfiles similares e infieren nuestros gustos.

Así, por ejemplo, un buen amigo ha comprado sólo libros en Amazon, y sin embargo le sugieren que compre algunos discos que casi siempre van con sus gustos y que en realidad fueron consultados o adquiridos por personas que tienen un perfil semejante en sus gustos respecto a libros.

Si revisamos la política de privacidad de Amazon, veremos que son muy cuidadosos en no dar datos concretos. Así, dicen "*Información de otras fuentes:* Podría

La privacidad en realidad no existe en Internet. La pregunta relevante es, ¿qué debemos hacer para lograr al menos una mínima protección?

mos recibir información sobre usted desde otras fuentes y añadirla a nuestra información de su cuenta". En los ejemplos que dan incluyen los términos que uno ha usado en buscadores como Alexa y A9.com, e información crediticia proveniente de los burós de crédito. Por cierto, esto último requiere en México de una autorización por escrito, de otra manera es ilegal (Ley para regular las sociedades de información crediticia, artículo 28), pero a nadie parece importarle. También resulta significativo que un cliente no pueda ver toda la información sobre sí mismo que Amazon tiene sobre él.

Si ligamos la cantidad de información que tienen las tiendas como Amazon con el artículo de los investigadores de la Universidad de Texas, no sería difícil que obtuvieran información delicada, como nuestras inclinaciones políticas. Lo importante de este asunto es que en ningún momento ponen límites al uso de dicha información, es decir, ejemplifican *algunos* de los usos que pueden dar a la información, pero no indican que no darán ningún otro uso.

Google y minería de datos

El nuevo gigante de la computación sin duda es Google que, además de operar el buscador más completo de Internet, ofrece numerosos servicios.

Google deposita en el navegador de sus visitantes una galleta o *cookie*, que no es otra cosa que un identi-

ficador que luego puede ligar con los datos personales de cada persona. Esta *cookie* tiene una caducidad de dos años. Ahora bien, el negocio de Google es la publicidad, y la mayoría de los sitios comerciales están afiliados a los programas publicitarios de Google. Esto significa que esta empresa no sólo puede guardar los términos de las búsquedas que uno hace, sino que también puede saber por dónde navega y en algún momento ligarla a información de nuestra persona, obtenida al inscribirse a algún servicio o hacer algún pago (si en una página de web usted oprime el botón derecho de su ratón, puede ver el "código fuente" de la página. Si en ella encuentra la palabra "googleadservices", esa página está afiliada a Google). La cantidad de información que tiene Google sobre los internautas es impresionante, y obviamente permite atar cabos y deducir muchas cosas de uno.

¿Qué información sobre los internautas tienen las agencias de espionaje? Con seguridad, nadie lo sabe en detalle, pero es muy probable que lo que hacen Google, Amazon, Microsoft Network (MSN) y los demás palidezca ante lo que tienen las organizaciones ligadas al espionaje.

Desde hace ya tiempo el gobierno de Estados Unidos revisa en forma continua el tráfico que pasa por Internet dentro de su territorio, y que incluye tanto tráfico doméstico como internacional. La cantidad de información que reciben es verdaderamente enorme, y por ello usan supercomputadoras que realizan *minería de datos* (véase el artículo "Minería de datos: cómo hallar una aguja en un pajar", de Gilberto Martínez, en este mismo número de *Ciencia*), la cual les permite separar lo trivial de lo interesante. Desde luego la pregunta es: ¿qué les interesa? Es algo que no podemos contestar con precisión. Obviamente, existe información asociada a los ataques terroristas que debe ver el personal de *Homeland Security* (Seguridad Interna) y seguramente comunicaciones del crimen organizado, pero ¿qué más? ¿Van a usar esa información para negar visas o con fines políticos? ¿Comparten esa información con otros gobiernos o partidos políticos de otros países? ¿Podría el personal que opera esta red de espionaje utilizarla para chantajearnos? ¿Hay un mercado negro en el que se venda esa información? ¿La están usando para descubrir, por ejemplo, quién proporciona información a Wikileaks (el famoso sitio web que publica informes anónimos y documentos filtrados con contenido sensible en materia de interés público)? Tal vez, no sabemos la respuesta a éstas y otras preguntas similares. Pero es claro que tienen la posibilidad de saber más de nosotros que lo que nosotros mismos podríamos escribir en un libro autobiográfico.

Este tipo de información también se usa para cometer el delito de "robo de identidad", hoy tan en boga.

En resumen, la privacidad en realidad no existe en Internet. La pregunta relevante es, ¿qué debemos hacer para lograr al menos una mínima protección? Por ello, en el resto de este artículo presentaremos una serie de recomendaciones útiles para lograrlo.

Segmente la información

No es conveniente tener toda nuestra información junta. Si bien una buena minería de datos puede juntar la información dispersa, a una persona común y corriente le costaría mucho trabajo, tanto que difícilmente lo intentará.

Para segmentar la información, abra varias cuentas de Facebook y otras redes sociales. En una cuenta maneje sólo aspectos formales, por ejemplo de negocios o de estudios. No ponga ahí nada que indique sus preferencias políticas ni otras informaciones que pudieran espantar a un empleador potencial. Cuando vaya a una entrevista de trabajo o alguna reunión de carácter formal ofrezca esta cuenta. Esto hará que en muchos casos ya no busquen la información de sus otras cuentas.

Use otra cuenta para aspectos familiares. Ábrala bajo el diminutivo o sobrenombre con que le conozcan en su familia y nunca con su nombre completo. Ni siquiera ponga sus apellidos.

Abra más cuentas para sus grupos de amigos, todas con seudónimos. Al menos una debe ser para amigos no muy cercanos a los que no les confiaría sus secretos. Abra otra para sus amigos cercanos, pero nunca ponga en ella ningún secreto, ésos hay que manejarlos en persona.

En todas las cuentas bloquee la información que terceros pueden añadir, como las etiquetas o *tags* en las fotografías de Facebook.

Cuando abra las cuentas en las redes sociales va a tener que dar un correo electrónico. Nunca use el mismo para las diversas cuentas ya que con él es trivial conocer todas las cuentas que tiene. Puede usar correos de hotmail, gmail, etcétera.

Haga lo mismo en sus cuentas de *chat*, en las que el ambiente informal y en tiempo real es propicio para "soltar" información que no debería.

Cuide su correo

Revise bien cada mensaje de correo electrónico antes de oprimir el botón de envío. Tome en cuenta que aunque usted sea cuidadoso, el receptor del correo lo puede reenviar, y fácilmente perderá el control de su información.

Aunque se supone que cifrar (poner en clave) el correo es una herramienta que evita que los administradores de los servidores de correo lean los suyos, puede meterlo en problemas serios. Es muy sencillo detectar en una computadora que analiza el tráfico cuáles correos están cifrados. Tome en cuenta que un correo cifrado automáticamente lo hace sospechoso de alguna actividad ilegal, desde crimen organizado hasta terrorismo. Si manda correo cifrado, no proteste porque le nieguen una visa para visitar Estados Unidos, y recuerde que buena parte del tráfico doméstico de México pasa por ese país cuando no hay comunicación directa entre las computadoras de origen y destino, cosa común cuando ambas están conectadas a diferentes redes de proveedores (en particular, si usa servicios de correo como hotmail, gmail, yahoo, etcétera, sepa que los servidores de correo están en Estados Unidos).

Configure correctamente su navegador

Buena parte de la fuga de información se da en los navegadores. Aunque es posible configurar correctamente los principales navegadores, es preferible usar alguno que no esté ligado a los servicios de búsqueda en Internet (como *Chrome*, de Google, e *Internet explorer*, de Microsoft, que está ligado a MSN) y evitar así un conflicto de intereses por parte del proveedor del navegador. Los principales navegadores independientes son *Opera* y *Firefox*.

Aquí especificaremos los pasos que hay que dar para configurar *Firefox* para una navegación razonablemente segura; en los demás navegadores los pasos son similares.

Lo primero que debemos hacer es que su navegador borre las *cookies* que ya tiene almacenadas. En *Firefox* hay que entrar a la opción "Privacidad" del menú "Preferencias". La opción por *default* será "Recordar el historial"; hay que cambiarla a "Usar una configuración personalizada para el historial". En ese momento aparecen una serie de opciones que debemos configurar. Hay que quitar la marca en "Modo permanente de navegación privada" y también las marcas en todas las líneas que dicen "Recordar...". Marcar "Permitir" y "Mantener", y en donde dice "Hasta que:" marcar "cierre *Firefox*". También hay que marcar "Limpiar el historial cuando *Firefox* se cierre" (si usa *Internet*

Explorer con su configuración básica, puede ver una demostración de fuga de información en: www.check-history.com/).

Ahora debemos oprimir el botón "Mostrar cookies" y aparecerá la lista de *cookies* que ya están guardadas. Por curiosidad puede ver las *cookies* que ya tiene. Están agrupadas por sitio, y se pueden ver oprimiendo la marca a la izquierda del sitio. Observará que en muchos casos aparecen *cookies* denominadas "__utmz", "__utma", "__utmc" y "__utmv", que son las de los sitios afiliados a Google.

Satisfecha nuestra curiosidad, debemos oprimir el botón "Eliminar todo", que quitará todas las *cookies*. Cerramos dos ventanas y quedamos en la ventana de "Preferencias". Ahí hay que ir a la pestaña "Seguridad", donde hay que quitar las marcas en "Recordar contraseñas de sitios web" y "Usar una contraseña maestra". Luego oprimimos el botón "Contraseñas guardadas", y si hay alguna la borramos con el botón "Eliminar todos".

Ya hemos terminado la configuración, así que podemos cerrar todas las ventanas de configuración.

Segmente su navegación

Con la configuración anterior lo podrán rastrear dentro de una misma sesión de su navegador, pero no podrán ligar dos sesiones una con otra, porque las *cookies* se destruyen al terminar la primera sesión. Si está participando en un debate político a través de visitas a *blogs* o poniendo comentarios en algún lado, y no quiere que liguen sus preferencias con su persona, cierre la sesión antes de entrar a sitios que lo puedan identificar más fácilmente, como tiendas o correos electrónicos.

Cuide la información que lo puede identificar

Las fotos que usted pone pueden ser usadas en su contra. Si tiene dinero, no le facilite la identificación a secuestradores ni les permita conocer su riqueza posando frente a su Porsche último modelo. Tampoco haga bromas de mal gusto como la que recientemente ocurrió cuando unos amigos pusieron fotos de un joven bajacaliforniano y su novia con el nombre de un narcotraficante y que luego, erróneamente, aparecieron entre las fotos de narcotraficantes de la Procuraduría General de la República (PGR). Esta broma le pudo costar la vida, o por lo menos un enorme lío legal, a este joven.

Otros problemas

La pérdida de privacidad es sin duda el problema de seguridad más serio que tenemos en Internet, debido a su volumen y universalidad. Sin embargo, hay otros problemas más tradicionales que también debemos cuidar.

Virus

Los virus de computadora son como una enorme nube de mosquitos que no nos deja en paz. Muchas veces su picadura –la entrada en nuestra máquina– no tiene grandes consecuencias; pero otras veces, como ocurre con el mosquito *Anopheles*, portador de la malaria, el virus de computadora trae dentro alguna mala sorpresa.

Los daños causados por los virus varían, desde bromas y borrado de archivos hasta programas que pueden ser usados para cometer delitos en nombre del usuario de la computadora.

Con frecuencia, los virus se usan para convertir una máquina en lo que en la jerga computacional se conoce como un *bot* (de "robot", ya que permite el control remoto de la máquina). Un bot consiste en un programa que puede recibir remotamente información e instrucciones para hacer cualquier tarea que se le ocurra al delincuente que lo controla (el "pastor" de un "rebaño" de bots).

Si bien nos va, cuando nuestra máquina ha sido convertida en *bot* por un virus que contrajo, va a ser usada para distribuir *spami*, o correo no deseado. Pero en otros casos puede usarse para delitos como atacar otros servidores –ya han sido bloqueados sitios como Facebook y Twitter con este método– o para distribuir programas pirata. O peor aún, para vender pornografía infantil.

Lo peor del caso es que, luego del delito, para el pastor es relativamente fácil borrar en nuestra máquina cualquier información que lo pueda identificar, así que quien carga el delito es el usuario.

La eliminación de los virus, todos ellos, es una tarea de seguridad importante. El enfoque, popular hasta ahora ha sido el de los programas antivirus, mal llamados "vacunas", que eliminan la mayoría de los virus. Este enfoque, sin embargo, tiene sus limitaciones.

Muchos virus no se pueden eliminar sin producir efectos secundarios, como pérdida de funcionalidad. Los virus nuevos, que aún no han sido catalogados por las empresas de antivirus, entran en las máquinas sin ser detectados, y son los que dan más problemas. Ha habido virus (como el famoso "Slammer"; http://en.wikipedia.org/wiki/SQL_slammer_worm) que en diez minutos han atacado la totalidad de sus víctimas potenciales en Internet sin dar la más mínima oportunidad a que las empresas de antivirus los cataloguen y repartan la versión actualizada correspondiente del programa antivirus a sus clientes. Por otro lado, la simple presencia del programa antivirus puede hacer que la velocidad de su máquina sea tan baja que le hace sentir a uno que está en la edad de piedra. Para colmo, se tiene que pagar continuamente para mantener el antivirus actualizado, un gran negocio para las empresas que los fabrican.

La inmensa mayoría de los virus han sido desarrollados para la plataforma Windows, de Microsoft. Hay varias razones para ello. El hacedor de virus busca que su "criatura" alcance el número máximo de máquinas, cosa que le facilita el casi monopolio de Microsoft. La estructura del núcleo del sistema operativo Windows, llamada "de *microkernel*", es otro factor que facilita hacer virus para ese sistema operativo. También es la plataforma más conocida desde el punto de vista de programación, de manera que hay muchos más delincuentes que la manejan, en comparación con otras plataformas.

En sistemas operativos como el MacOS, de las máquinas Macintosh de Apple, y el UNIX, con todas sus variantes, incluido el Linux, casi no hay virus, y los pocos que existen no dan problemas incluso sin la protección de un antivirus, entre otras cosas porque para que un virus se propague se necesita el contacto entre máquinas del mismo tipo, cosa que ocurre pocas veces en plataformas que no sean Windows.

He aquí algunas recomendaciones para reducir el problema de los virus:

Considere cambiar de plataforma. Puede mudarse a una "Mac", o si no quiere comprar otra máquina, instale

Linux en su PC. Puede instalarlo sin quitar Windows, "por lo que pudiera ofrecerse". La versión de Linux más recomendable es Ubuntu (www.ubuntu.com). Ésta es sin duda la mejor opción contra los virus.

Mantenga actualizado su antivirus. Si no puede cambiar de plataforma, no le queda de otra que aguantar los problemas que causan los antivirus. Esto implica costo, y mantener un antivirus en su máquina la hará más lenta. Tampoco estará exento por completo de los problemas causados por los virus.

Corte por lo sano cuando lo invada un virus. Aun con un antivirus actualizado en una máquina Windows, va a tener infecciones. Cuando esto ocurra, si el virus no es nuevo, el antivirus le dirá que si lo quiere eliminar. Con mucha frecuencia la limpieza que realizan este tipo de productos resulta incompleta o genera otros problemas, así que a la primera anormalidad después de que su antivirus hizo una limpieza, no dude en hacer un respaldo de sus documentos y otros datos, *sin respaldar programas*, formatear el disco y cargar de nuevo todo desde los CD originales; finalmente, reconstruya sus datos. Si el virus es nuevo, no tendrá otra alternativa que ésta.

Espionaje

Independientemente de los problemas de privacidad ya mencionados, existe la posibilidad de que en su computadora entren programas que espíen sus actividades. Éstos pueden llegar al visitar un sitio de Internet que los instala en forma de una barra de navegación para su navegador favorito, o como anexos en un correo electrónico, o simplemente alguien cercano puede instalarlos cuando tiene acceso físico a su máquina.

Típicamente, estos programas monitorean el teclado de la computadora y la barra de direcciones del navegador, y son capaces de enviar al correo electrónico del atacante, o a un sitio de Internet, todo lo que ha tecleado, así como archivos suyos, frecuentemente todos los que están en la carpeta de documentos.

Para prevenir este tipo de problemas le recomendamos:

Proteja el acceso a su computadora con una contraseña. Se pueden definir contraseñas para iniciar la sesión cuando arranca la máquina, o en un protector de pantalla, para cuando no haya actividad. Asegúrese de activar el protector de pantalla cada vez que se levante de la computadora, así sea sólo por unos minutos.

Nunca permita la instalación de barras de navegación. Supuestamente las barras de navegación que se instalan en los navegadores están hechas para hacerle la vida más fácil; sin embargo, hay muchas que ocultan *software* malicioso o que simplemente están hechas para reportar sus actividades a sitios que venden información de mercadotecnia.

Phishing

Los estafadores no podían resistir la tentación de usar Internet para hacer fraudes, e inventaron lo que en el inframundo del ciberespacio llaman "*phishing*" (del inglés *fishing*, salir de pesca).

Se trata en realidad de una técnica muy vieja, en la que se hace aparecer una pantalla falsa que es prácticamente idéntica a la real, para recabar en ella información de las víctimas.

En su forma moderna, consiste en que uno recibe un correo electrónico que aparentemente proviene de su banco u otra institución, en el que le piden que visite una cierta página con el fin de hacer cosas como actualizar los datos o evitar que le cancelen una cuenta, y le dan una liga que, al ser oprimida, lo lleva a un sitio que tiene toda la apariencia de ser el sitio original.

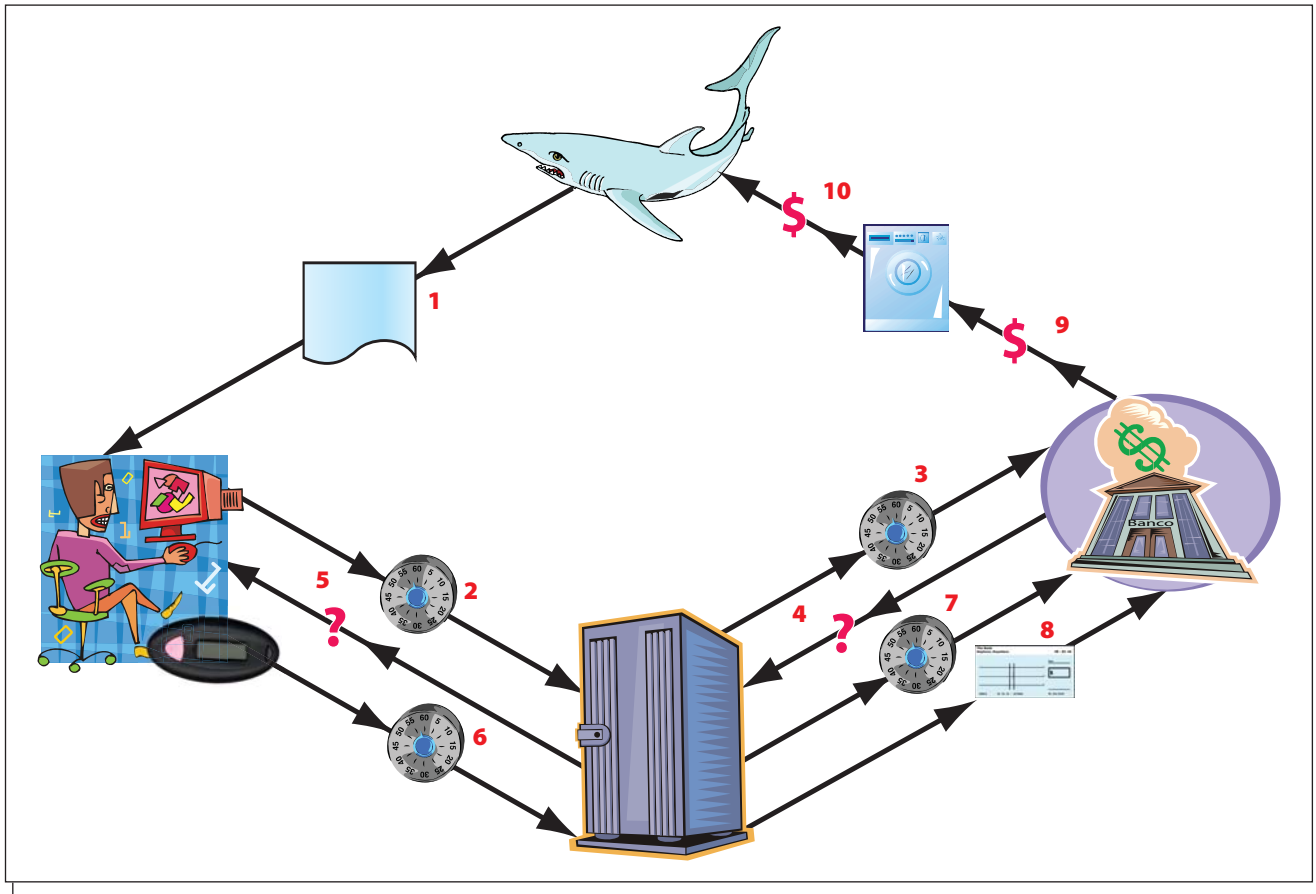

Figura 1. Diagrama del *phishing*.

Con frecuencia estos sitios, llamados "*fakes*" (falsificaciones), son copias tan perfectas que no podemos distinguirlas de los originales, y usan incluso las imágenes y otros elementos tomados directamente del sitio original.

Los bancos han reaccionado a esto dándole a sus clientes un *token* o dispositivo de claves dinámicas. Ya sea por tiempo, o con un número que cada vez manda el banco, y que se debe teclear en el dispositivo, o consultando una tabla que se proporciona en una tarjeta, la idea fue tener un identificador efímero que asegure que el cliente está en posesión física de un dispositivo, en adición a las tradicionales contraseñas.

En un principio esta estrategia funcionó: si usted daba información al atacante en el sitio *fake*, ésta no le servía, porque no tenía manera de obtener la información dinámica. Pero siento darle una mala noticia: los estafadores rápidamente resolvieron ese problema. Hoy, cuando usted se conecta al sitio *fake*, hay un programa de computadora detrás que en ese momento se conecta al banco. Usted usa su número de cuenta y contraseña, y el programa se los da al banco. Luego el banco le pide al programa del atacante la información dinámica y el programa se la pide a usted. Cuando usted la proporciona, el programa se la envía al banco, y queda abierta una sesión en la que hace el fraude automáticamente. El atacante ni siquiera tiene que gastar tiempo recibiendo información y haciendo los fraudes manualmente: simplemente se sienta en un sillón cómodo a ver la televisión mientras las cuentas en que se recibe el producto de los fraudes se llenan solas.

Para disminuir los daños causados por el *phishing*, he aquí algunas recomendaciones:

Ignore por completo los correos de bancos y otros sitios similares. Ni siquiera abra esos correos, simplemente bórrelos. Si tiene duda de que en realidad el banco puede querer algo, entre a su cuenta en el sitio del banco, si era algo importante, ahí estará la información.

Teclee siempre la dirección del banco en el navegador. Nunca vaya a un sitio en el que se maneja dinero oprimiendo una liga en otro sitio o en un correo electrónico. Es trivial poner un letrero y dirigirlo a otro sitio.

Mantenga su dispositivo de claves dinámicas bajo llave. Esto no tiene mucho que ver con el *phishing*, pero evitará que alguien que haya averiguado sus contraseñas, por ejemplo viendo el teclado cuando las escribe, eche mano del dispositivo y le haga una mala jugada.

Hay muchos otros delitos que se cometen a través de Internet o de una computadora, pero son más bien asunto de los administradores de los servidores o las redes de comunicación.

En conclusión, las computadoras y las redes de comunicación digitales nos han proporcionado múltiples beneficios y no podríamos concebir la vida moderna sin ellas; sin embargo, también han traído riesgos nuevos que tenemos que tomar en cuenta para obtener de ellas el máximo beneficio.

Resumen de medidas de seguridad

Privacidad

- Segmente la información.
- Cuide su correo.
- Configure correctamente su navegador.
- Segmente su navegación.
- Cuide la información que lo puede identificar.

Virus

- Considere cambiar de plataforma.
- Mantenga actualizado su antivirus.
- Corte por lo sano cuando lo invada un virus.

Espionaje

- Proteja el acceso a su computadora con una contraseña.
- Nunca permita la instalación de barras de navegación.

Phishing

- Ignore por completo los correos de bancos y otros sitios similares.
- Teclee siempre la dirección del banco en el navegador.
- Mantenga su dispositivo de claves dinámicas bajo llave.

Guillermo M. Mallén Fullerton es egresado de la Facultad de Química de la Universidad Nacional Autónoma de México (UNAM). Es maestro en computación por la Universidad Iberoamericana. Ha publicado libros y artículos sobre temas de seguridad, y ha dirigido numerosas tesis de licenciatura y maestría. Ha presentado trabajos en diversos congresos nacionales e internacionales, y ha sido conferencista magistral en diversos congresos de seguridad. Ha participado en importantes proyectos de seguridad a nivel nacional. Es coautor del libro *Seguridad de la información*, el primero escrito en México sobre este tema. Actualmente es consultor privado y profesor de la Universidad Iberoamericana. Ha sido conferencista magistral sobre seguridad en diversos eventos. mallen@chispa.com.mx