

¿Es seguro comprar o pagar cuentas de manera Online?



Quizás una de las preguntas que más frecuentemente me corresponde contestar es: ¿Es seguro comprar o pagar cuentas por Internet?

Y me respuesta siempre ha sido la misma: si tomás un par de precauciones básicas, y el sitio tiene buena reputación, realizar una transacción por Internet (a través de páginas HTTPS) es más seguro que entregar la tarjeta de crédito en un bar.

Eso era hasta hace unos meses, cuando distintos hechos relacionados con robo de certificados digitales comenzaron a hacerse públicos, y no se han detenido hasta ahora.

¿Cómo funcionan los certificados digitales?

Un **certificado digital** es un documento digital firmado, a través de procesos criptográficos, por una entidad de confianza que actúa como notario y que verifica que un sitio web es quien dice ser. De esta forma por ejemplo, dicha entidad asegura a los usuarios, que el sitio web de un banco es real.

Cada vez que un usuario ingresa a un **'sitio web seguro'** a través de HTTPS, se utiliza un protocolo -SSL/TLS- que garantiza que el contenido del tráfico web sea cifrado y que, en teoría, nadie podría intervenir y acceder a dicho contenido, asegurando así la privacidad de la comunicación y de la información transmitida. Por otro lado, al acceder a dicho sitio, el navegador recibe el certificado digital y verifica que el mismo se encuentre firmado por una autoridad digital de confianza. Si las validaciones son correctas, el usuario tiene la garantía de que el sitio es real y seguro. En caso de no ser así, se muestra al usuario una advertencia.

Las empresas que ofrecen certificados digitales no son demasiadas y cada navegador tiene una lista de certificados raíz de confianza, lo que le permite realizar esta verificación en forma rápida y transparente para el usuario.

Como puede verse, el secreto radica en la entidad de confianza, ya que si alguien accede a sus certificados o fuera posible generar/falsificar los mismos, cualquiera podría impersonalizar a una empresa o producto, logrando que la confianza de todo el modelo sea utilizada como un arma y no como una herramienta de prevención de ataques. Por otro lado tampoco es posible dejar de confiar en todas las empresas de certificación porque, básicamente se estaría matando el modelo de navegación segura actual.

Inconvenientes que comenzaron a surgir con los Certificados Digitales:

En marzo pasado, la empresa Comodo, informó que 'una serie de certificados digitales habían sido emitidos sin una validación de identidad suficiente' [1], dando lugar a que empresas como Microsoft, Google, Yahoo!, Skype y Mozilla pudieran ser impersonalizadas y que, los usuarios corrieran el riesgo de ser engañados, simulando ser las importantes empresas mencionadas. Entre los posibles ataques se podrían realizar distintas acciones delictivas como: redirigir tráfico de Internet a servidores de delincuentes, recolectar información y contraseñas de usuarios y facilitar el robo de identidad.

Recientemente, en agosto la situación se repitió cuando la empresa Diginotar [2] 'perdió' cientos de certificados de organizaciones, empresas, gobiernos y organismos de control y vigilancia internacional [3], permitiendo que miles de ciudadanos iraníes hayan sido vigilados por un período de tiempo indeterminado y provocando incluso que la empresa deba ser intervenida por el gobierno holandés y que finalmente se viera obligada a cesar sus operaciones. Además siempre queda la duda (y la amenaza) sobre si otras entidades de certificación también pueden estar siendo atacadas.

Problemas implícitos del modelo de navegación actual:

El modelo descrito siempre ha tenido algunas deficiencias, que con el pasar del tiempo o con los robos de certificados digitales actuales se han profundizado, e incluso hace dudar sobre la confiabilidad de navegar en supuestos sitios seguros.

El primer problema radica en que si una organización o persona crea un sitio web seguro (HTTPS) pero utiliza sus propios certificados digitales (autofirmados) o utiliza los de una entidad no reconocida como tal por los navegadores, el usuario recibirá una advertencia, que podría ser confundida con la inseguridad del sitio:

- Relacionado a estas advertencias, aún si el sitio fuera inseguro y se presentaran las advertencias del caso, el usuario tiende a ignorar los mensajes, lo cual está relacionado con una fuerte falta de educación en seguridad de toda la comunidad.
- Por otro lado, en el mercado se pueden conseguir certificados digitales muy baratos o gratuitos o temporales y, si un delincuente decide utilizar estos certificados para crear un sitio falso, simulando ser una entidad de confianza, sería posible engañar a los usuarios sin que los mismos se percaten, hasta que sea demasiado tarde y su información ya haya sido comprometida [4]. En ESET Latinoamérica se puede ver un video sobre la utilización de estos certificados gratuitos y cómo es sencillo crear este tipo de escenarios [5].
- No existe ningún proceso que realmente dé confianza al usuario sobre una entidad u otra, sino que el modelo simplemente se basa en que si un navegador confía en un certificado, el usuario, por transición casi seguro también lo hará.
- En la práctica sucede que existen métodos y herramientas por las cuales es posible intervenir una comunicación y robar información sensible, por más que la misma se realice a través de un canal HTTPS y el usuario haya verificado que efectivamente dicha comunicación sea "segura".
- Este modelo de seguridad nunca funciona en los casos en que el usuario tenga instalado algún programa dañino (malware) en su sistema, por lo cual, decir que "si estás sobre HTTPS estás seguro" en realidad es una falsa sensación de seguridad.
- Recientemente se han publicado algunos trabajos de investigación que mencionan y explotan vulnerabilidades en algunas versiones de los protocolos SSL y TLS y que podrían dar lugar a ataques desconocidos hasta el momento contra entidades de confianza y la información que se intercambia, aun cuando todo el modelo de certificación sea verdadero. Otros estudios van más allá y, directamente aseguran que ya es tiempo de cambiar el modelo de certificación.

Además de estos problemas implícitos en el modelo y los protocolos, recién hace muy poco, sitios muy populares y visitados como webmails y redes sociales incorporaron la autenticación a través de HTTPS ya que, anteriormente muchos de ellos enviaban la información sensible del usuario a través de HTTP, en texto claro (algunos aún lo hacen). Este problema en realidad no es un error del modelo de certificación, sino de la implementación o falta de ella por entidades y empresas irresponsables.

Pero, amén de lo expresado, la situación actual más preocupante es que diferentes entidades certificadoras de confianza han visto vulneradas sus infraestructuras, a través de distintos ataques y fuga de información, y se han comprometido los certificados digitales de cientos de empresas y organismos internacionales.

El problema es complejo, los delincuentes no pierden tiempo y nuestra información sensible es cada vez más buscada. Estas situaciones dan lugar para comenzar a ser más cuidadosos y a estar atentos sobre estos temas y hacen que ya no sea tan trivial recomendar: "Navegá sobre HTTPS porque de esa manera tu información estará segura".

Una vez más, **la educación como medida de seguridad se vuelve imprescindible.**

[1] Microsoft advierte que certificados fraudulentos emitidos por Comodo permitirían ataques

<http://blog.segu-info.com.ar/2011/03/microsoft-advierte-que-certificados.html>

[2] Diginotar

<http://en.wikipedia.org/wiki/DigiNotar>

[3] Consiguen certificados SSL falsos de la CIA, MI6, Mosad y otros

<http://blog.segu-info.com.ar/2011/09/consiguen-certificados-ssl-falsos-de-la.html>

[4] Cazando mitos: HTTPS

<http://blogs.eset-la.com/laboratorio/2009/10/02/mito-https/>

[5] Video sobre certificados gratuitos y sitios no confiables

http://www.youtube.com/watch?v=QhF_8uVNrX4

Autor: Cristian Borghello

Fuente: ZMA