Riesgos de los pagos móviles

Tras los dos posts anteriores en los que hemos tratado aspectos generales acerca de los pagos móviles, en este nos vamos a centrar en uno de los temas que más nos pueden llegar a afectar, los posibles riesgos a los que estamos expuestos a la hora de utilizar dicha tecnología. Por ello, algunas de las preguntas a las que vamos a poner respuesta son las siguientes: ¿cuáles son los riesgos a los que estamos expuestos?, ¿qué tipo de pérdidas podemos sufrir en caso de ser hackeados? Es obvio que, tal y como yo hago, estamos constantemente adquiriendo productos vía móvil, de hecho, según informan algunos medios de comunicación, más de la mitad de los ciudadanos realizamos compras de manera semanal o incluso diaria. Es por esa razón que el uso de la banca móvil ha sufrido un gran incremento con el paso de los años, según una encuesta realizada por ISACA en 2015, el 87% de los 900 encuestados practicantes de la seguridad estimaron un aumento del uso de esta tecnología, y debemos concienciar y alertar a los usuarios de los posibles riesgos que pueden producirse [1].

En primer lugar, todos nuestros dispositivos móviles cuentan con una serie de sistemas de seguridad que nos protegen de los distintos riesgos que nos rodean, ya sean los sistemas de seguridad de pagos, usuarios, comunicación o de puntos finales, sin embargo, se han dado ciertos casos en los que hackers han podido traspasar esas barreras y causar graves problemas en la ciudadanía. De hecho, tal y como afirma el 47% de encuestados en la investigación de ISACA, los pagos móviles no son 100% seguros, estamos totalmente expuestos a diversos riesgos tanto controlables como no controlables por nosotros mismos que procederé a enumerar más adelante. Algunos de los sistemas de seguridad más importantes son la autenticación de dos factores, la tokenización, concepto que hace referencia al envío de señales aleatorias al punto de venta y la red de pago y los criptogramas, encargados de garantizar que los pagos móviles sean únicamente utilizados desde el propio dispositivo del usuario [2].

Algunos de los riegos de los pagos móviles:

Como bien os he comentado en reiteradas ocasiones, el uso de los dispositivos móviles para realizar pagos ha supuesto un incremento de los robos debidos a los riesgos que estos conllevan. Entre ellos encontramos dos claros tipos de

objetivos que son frecuentemente perseguidos. A continuación, mostraré una ilustración donde se muestran los tipos de amenazas y riesgos que tienen lugar cuando hacemos uso de dicha tecnología, así como la escala (del 1 al 3) de probabilidad e impacto de estos:

Tipo de objetivo perseguido	Amenazas	Riesgos	Probabilidad	Impacto
Usuario	Intercepción del tráfico	Robo de identidad	Baja	3
Usuario	Intercepción de datos de autenticación	Robo de parámetros de autenticación, divulgación de información confidencial	Moderada	3
Usuario	Enmascaramiento del usuario	Transacciones fraudulentas	Moderada	2
Usuario	Configuración y complejidad de configuración	Reducción en la adopción de la tecnología	Baja	1
Usuario	Infección del dispositivo móvil	Divulgación de datos y violación de la privacidad	Moderada	2
Proveedor de servicio	Ataques enmascarados	Robo de servicios y modificación de mensajes	Baja	2
Proveedor de servicio	Distribución ilegal de contenido como videos o juegos.	Robo de contenido, piratería digital.	Baja	2
Proveedor de servicio	Modificación de mensajes, respuesta de transacciones.	Robo de servicio o contenido, pérdida de ingresos, transferencia ilegal de fondos	Moderada	3

Riesgos de la tecnología empleada

A todo lo anterior se le suman los riesgos producidos por el uso de tecnologías como NFC, tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia. Conocemos a NFC como una de las más cómodas y seguras de la actualidad, no obstante, éstos no son invulnerables y la seguridad depende, como en la mayoría de las cosas, del uso que hagamos de ello. Por ello, viene bien que os comenté los peligros de estos sistemas de pago de manera que todos hagamos un correcto y seguro uso de ello.

Las escuchas de piratas informáticos son una de las principales amenazas a

tener en cuenta ya que, a pesar de que sea complicado de que se den esos casos, nuestro smartphone se encuentra constantemente intercambiando datos bancarios, lo que podría ser interceptado por este tipo de personas y utilizarla para averiguar información de los usuarios.

Otro de los riesgos a los que estamos sometidos y que no dependen de nosotros reside en los posibles fallos de seguridad de los que disponen algunas de las aplicaciones de pago existentes en el mercado. Exactamente igual que en el caso anterior, si eso ocurre podría suponer un grave peligro para nuestra seguridad.

El uso del PIN del propio dispositivo móvil es uno de los mecanismos que más nos pueden ayudar a disipar los riesgos. En caso de carecer de ello, cualquier persona que se apropie de nuestros smartphones podrá acceder a las aplicaciones y obtener nuestra más personal y confidencial información. Por esa razón, muchas aplicaciones bancarias relacionadas con los pagos móviles ya implementan el uso de la propia huella digital como mecanismo para controlar este tipo de riesgos.

La activación constante del NFC en nuestros dispositivos también puede suponer que un hacker intercepte nuestro chip y se comunique con el haciéndose pasar por un sistema de pago normal y corriente para conseguir nuestros datos bancarios.

El último de los riesgos que procedo a comentar tiene una probabilidad de ocurrencia media, no obstante, el impacto que éste supone es increíble (podríamos tratarlo como nivel 3). Hablo sobre el robo de los dispositivos móviles, acción que vemos como aumenta de manera considerable con el paso del tiempo y que, ya que ahora es posible el pago sin contacto, se convierten en interesantes objetivos para los ladrones [3].

Me gustaría concluir el presente post animando a todos los usuarios a que lean la siguiente entrada que se publicará en el blog dado que trataré algunas de las mejores técnicas para poder disipar los riesgos existentes al utilizar estas técnicas. Asimismo, trataré de completar el cuadro adjuntado en la parte superior de manera que se listen todos los planes de contingencia pertinentes a los riesgos indicados. Espero que os haya servido para concienciaros acerca del tema y que lo tengáis en cuenta ya que están en juego nuestras tarjetas bancarias e información más privada.

Bibliografía

[1] Mobile Payments: Risk, Security and Assurance Issues. Acceso el 06/10/18. https://www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/MobilePaymentsWP.pdf

[2] ISACA Challenges Mobile Payment Security Perceptions. Acceso el 06/10/18. https://www.isaca.org/About-ISACA/Press-room/News-Releases/2016/Pages/ISACA-Challenges-Mobile-Payment-Security-Perceptions.aspx

[3] Que es el NFC que están poniendo en las tarjetas de crédito. Ventajas y

peligros. Acceso el 07/10/18. https://www.smythsys.es/6369/que-es-el-nfc-que-estan-poniendo-en-las-tarjetas-de-credito-ventajas-y-peligros/