ZIMPERIUM®

5 consejos para proteger su aplicación retail y su negocio

Proteja su aplicación retail

La crisis del COVID-19 ha cambiado la forma de consumir bienes físicos y digitales. Los comercios retail han tenido que cambiar rápidamente su forma de operar.

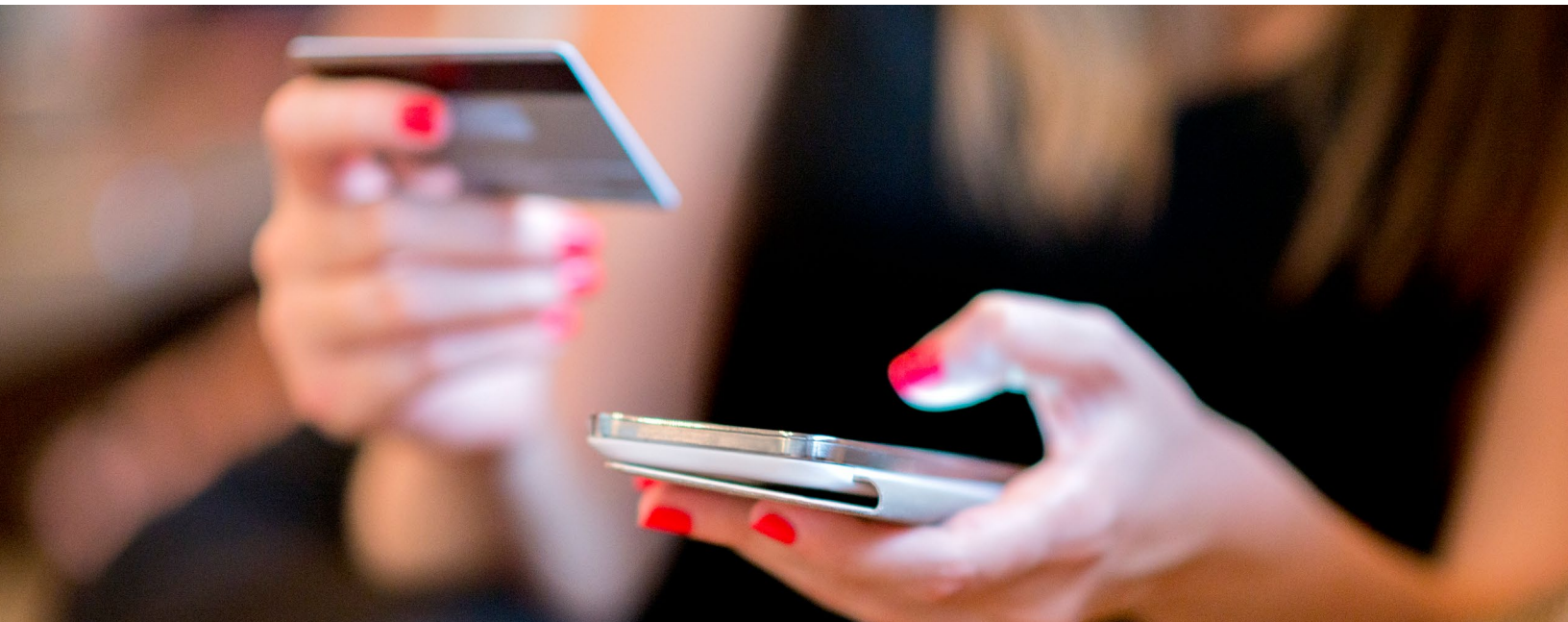
Para los retailers, la necesidad de un medio seguro y sin contacto para navegar y comprar a través de las aplicaciones móviles se ha convertido en algo fundamental para su supervivencia. Las marcas online y en plataformas de eCommerce crecieron enormemente durante la pandemia. Los ingresos netos de Amazon en el primer trimestre de 2021 aumentaron un 224% respecto al mismo periodo del año anterior, y las ventas de Target en 2020 crecieron un 19,8%.

Se prevé que las ventas del comercio móvil alcancen los 3,56 billones de dólares en 2021, un 22,3% más que los 2,91 billones que registró en 2020. Con el número de usuarios de móviles actualmente en 5,22 millones y en aumento, nada indica que el crecimiento del comercio móvil vaya a detenerse pronto. Sin embargo, este cambio en los comportamientos de compra sigue dejando al descubierto múltiples brechas de seguridad en las aplicaciones móviles de los comercios, sobre todo porque casi todas ellas permiten realizar pagos desde la aplicación.

Fallos de seguridad en la aplicación de venta retail

El mayor impulsor del crecimiento del comercio móvil es la conveniencia de las compras realizadas desde el móvil. Poder elegir la forma de pago hace que la experiencia del usuario sea óptima. Tres de cada cuatro consumidores afirman que realizan las compras en sus dispositivos móviles porque les ahorra tiempo. Esta dinámica hace que los retailers impulsen constantemente nuevas aplicaciones y funciones, previas a los eventos de compra masivos. Pero este enfoque alocado y apresurado por vender resulta en dejar de dar prioridad a la seguridad por encima de otras características que conducirán a atraer más compradores y generar más ventas.

En un estudio de 2019, analizamos las versiones para Android e iOS de las 30 principales aplicaciones de compras móviles (60 aplicaciones en total) para entender cómo las mismas gestionan los riesgos de seguridad y privacidad de los usuarios. Descubrimos que todas las aplicaciones eran vulnerables a la ingeniería inversa que los atacantes utilizan para crear aplicaciones fraudulentas. Además, el 92% no protegía adecuadamente la comunicación de datos sensibles, el 70% no protegía adecuadamente el almacenamiento de datos sensibles y el 48% era vulnerable a la manipulación del código...



Cómo los ciberdelincuentes atacan las aplicaciones de compra

Las aplicaciones de los comercios que no se adhieran a las mejores prácticas de seguridad son el principal objetivo de los ciberdelincuentes durante las fiestas. Una encuesta reciente de la empresa de informes crediticios Experian reveló que casi una cuarta parte de los encuestados había sido víctima de un robo de identidad o de un fraude durante las fiestas anteriores.

Hay varias formas en las que los actores fraudulentos pueden utilizar los fallos de seguridad de las aplicaciones retail para robar datos o redirigir los pagos. Un buen ejemplo es la creación de aplicaciones falsas que se parecen a las reales. Veamos, con más detalle, cómo funciona esto:

Paso 1
Los ciberdelincuentes descargan aplicaciones legítimas de Google Play o Apple App Store, las descompilan y realizan ingeniería inversa del código fuente para entender cómo funciona la aplicación.

Paso 2
Los ciberdelincuentes utilizan este código para crear versiones copiadas, de aspecto casi idéntico al original, pero con código fraudulento insertado. El código fraudulento se salta los controles de seguridad y validación, captura las pulsaciones del teclado, roba y extrae información, etc.

Paso 3
Los ciberdelincuentes publican las aplicaciones copiadas en sitios web y tiendas de terceros y las promocionan mediante campañas de ingeniería social. Los consumidores incautos son víctimas, las descargan y las instalan.

Una vez instaladas, toda la información introducida va directamente a los ciberdelincuentes.

La creación de aplicaciones de imitación no es una tendencia nueva ni mucho menos. Un informe de 2019 de RiskIQ descubrió casi 1.000 aplicaciones fraudulentas relacionadas con las compras navideñas y otras 6.000 aplicaciones que se aprovecharon de marcas de minoristas de confianza para atraer a las víctimas.

La escasa seguridad de las aplicaciones facilita que los delincuentes estafen a los clientes, especialmente a los que se aventuran a comprar en línea por primera vez debido a la pandemia. Para las organizaciones, esto supone una pérdida de ventas, un grave daño a la confianza de los consumidores e incluso posibles litigios o multas reglamentarias.

Consejos para mejorar la seguridad de las aplicaciones de los comercios

Las compras en línea son ya una forma de vida. Pero los clientes esperan que los comercios protejan sus datos personales y los de sus tarjetas de pago. Cuando las aplicaciones se ven comprometidas, se rompe la confianza de los clientes. Y los retailers son muy conscientes de que la confianza es clave para que los consumidores gasten en su marca. La buena noticia es que los desarrolladores de aplicaciones tienen muchas opciones cuando se trata de crear una aplicación segura, compatible, y resistente frente a una amplia variedad de ataques.

Ofuscación avanzada de código

La ofuscación es el proceso de transformar el código para dificultar su comprensión y análisis por parte de los hackers, pero de forma que siga siendo totalmente funcional. Si bien no detendrá por completo a los atacantes muy decididos, la ofuscación avanzada de código hace que las cosas sean tan costosas, y requieran tanto tiempo, que no les merezca la pena continuar.

Detección de Rooting/ Jailbreak

El rooting y el jailbreak alteran la integridad de un dispositivo móvil para eludir los controles de seguridad del sistema operativo y del dispositivo establecidos por Google y Apple. Los usuarios de móviles lo hacen por razones perfectamente inocentes. Sin embargo, si su aplicación de compras se ejecuta en un entorno de este tipo, cualquier aplicación fraudulenta podría acceder a su aplicación, sus datos, credenciales y claves criptográficas. Las aplicaciones deberían tener la capacidad de detectar un dispositivo con jailbreak o rooteado y tomar acciones defensivas en consecuencia.

Mecanismos antisabotaje

Los ciberdelincuentes manipulan las aplicaciones para alterar su funcionamiento. Por ejemplo, para pedir información confidencial, instalar rootkits y puertas traseras, desactivar la supervisión de la seguridad, insertar programas fraudulentos para robar información o secuestrar la aplicación para algo no previsto. El sistema antisabotaje detecta las modificaciones no autorizadas del código, mediante técnicas como la comprobación de la integridad y, por lo general, desencadena una respuesta de defensa como el bloqueo del acceso a la cuenta o el cierre de la aplicación.

Criptografía de caja blanca

Cuando los hackers no pueden romper los algoritmos criptográficos que protegen la información privada de los clientes, se centran en robar las claves para descifrarla. Los dispositivos móviles ofrecen almacenes de claves para guardar y utilizar de forma segura las claves criptográficas (Android Keystore, Apple Secure Enclave). Se trata de mecanismos de protección que dependen del hardware. Pero la falta de estandarización entre los dispositivos significa que los niveles de protección pueden variar, y el propio sistema operativo móvil y los almacenes de claves pueden tener fallos de seguridad. Por ejemplo, el pasado mes de julio, unos piratas informáticos descubrieron una vulnerabilidad permanente en el procesador Apple Secure Enclave.
La criptografía de caja blanca es una protección de claves criptográficas basada en software que presupone un ataque y una exposición. Utiliza una compleja ofuscación y transformaciones criptográficas para mantener las claves protegidas y ocultas en todo momento, incluso mientras se utilizan.

La seguridad debe ser su prioridad

Utilizar la seguridad más básica en la aplicación es muy importante. No almacene información crítica en el dispositivo a menos que sea necesario; asegúrese de que todos los datos que recibe la aplicación están sujetos a la validación de entrada; utilice métodos de cifrado robustos y asegúrese de su correcta implementación. Si debe almacenar contraseñas, protéjalas con estándares de cifrado fuertes y ampliamente aceptados. Y recuerde proteger también las claves criptográficas.

Cómo ayuda Zimperium a proteger las aplicaciones retail

La pandemia ha cambiado por completo ciertos comportamientos de compra de los consumidores. Navegar y comprar a través de aplicaciones móviles es la nueva normalidad. Las ventas de eCommerce móvil, como parte del total del eCommerce, aumentaron del 52,4% de la cuota de mercado en 2016 al 72,9% actual.

La suite de protección de aplicaciones de Zimperium permite a los retailers crear aplicaciones seguras y conformes con la normativa PCI que generan la confianza de los clientes. Para obtener más información, póngase en contacto con uno de nuestros expertos hoy mismo.

ZIMPERIUM®

zimperium.com
844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244