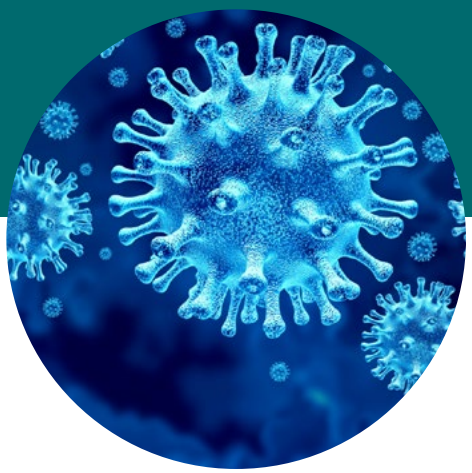
8 consejos para ayudar a los pequeños comerciantes a proteger los datos de tarjetas de pago



La pandemia del COVID-19 ha cambiado rápidamente la manera en que los pequeños comerciantes aceptan pagos. Los comerciantes que anteriormente solo tenían locales físicos empiezan a aceptar transacciones de comercio electrónico y por teléfono. PCI Security Standards Council comparte consideraciones fundamentales para ayudar a los pequeños comerciantes a mantener protegidos los datos de pago de sus clientes en este entorno en rápida evolución.

COMPRENDAMOS EL RIESGO

Los delincuentes cibernéticos actúan rápidamente para aprovecharse de los apresurados cambios en los entornos de datos de tarjetas de pago.

475% de aumento en los informes malintencionados en relación con el Coronavirus en marzo.[1]

41% de pequeñas empresas que sufrieron violación de datos pagaron más de $50,000 para recuperarse.[2]

29% de consumidores encuestados afirmaron que nunca más usarían los servicios de una empresa pequeña que sufrió una violación de datos.[3]

1: Fuente: BitDefender 2, 3: Fuente: Bank of America Small Business Payments Spotlight

CONSEJOS PARA PEQUEÑOS COMERCIANTES

Estos y otros recursos están disponibles en la página web de PCI SSC para Pequeños comerciantes y en el Blog PCI Perspectives.

CONSEJO NO. 1 REDUZCA LA CANTIDAD DE LUGARES DONDE SE PUEDEN ENCONTRAR DATOS DE TARJETAS DE PAGO

La mejor manera de protegerse contra las violaciones de datos es no almacenar para nada datos de tarjetas. Muchos pequeños comerciantes actualmente ofrecen recolección en ubicaciones adyacentes a la acera y aceptan pagos por teléfono en lugar de las transacciones cara a cara. Evite anotar los datos de las tarjetas de pago. En su lugar, ingréselos directamente a su terminal segura.

Más información: Artículo del Grupo de interés especial del PCI SSC: Cómo aceptar pagos vía telefónica de manera segura

CONSEJO NO. 2: USE CONTRASEÑAS SEGURAS

El uso de contraseñas no seguras y predeterminadas es una de las causas principales de la violación de datos de pago de las empresas. Para ser eficaces, las contraseñas deben ser seguras y actualizarse periódicamente. Las contraseñas no seguras y las predeterminadas por los proveedores son una fuente frecuente de violación de datos de pequeños comerciantes.

Más información: Infografía sobre contraseñas seguras

CONSEJO NO. 3: REVISE EL SOFTWARE, APLIQUE PARCHES Y MANTÉNGALO ACTUALIZADO

Los delincuentes buscan software obsoleto para explotar las fallas de sistemas que no tienen parches. La instalación oportuna de parches de seguridad es crucial para reducir el riesgo de que haya filtraciones. Una manera de mantenerse al día con todos los cambios necesarios es realizar análisis de vulnerabilidad para identificar problemas de seguridad. Los proveedores de análisis aprobados (ASV) por PCI pueden ayudarle a identificar vulnerabilidades y errores de configuración en sus sistemas de pago en línea, sitio web de comercio electrónico y otros sistemas, proporcionándole un informe de sus vulnerabilidades y la manera de resolverlas –por ejemplo, los parches que se deben aplicar–. Asegúrese de actuar de acuerdo con los resultados de los análisis de vulnerabilidad de los ASV y de mantener su software actualizado.

Más información: Infografía sobre aplicación de parches

PCI Security Standards Council

CONSEJO NO. 4: USE CIFRADO SÓLIDO

El cifrado hace que los datos de las tarjetas de pago sean ilegibles para personas que no cuentan con una clave específica, y se usa para proteger datos almacenados o datos transmitidos por la red. Pregunte a su proveedor si el cifrado de su terminal de pago se hace mediante cifrado de extremo a extremo (P2PE), y si está incluido en la lista del PCI SSC de soluciones de P2PE validadas por PCI. Si configurará un nuevo sitio web, confirme que el proveedor de carritos de compra utilice cifrado adecuado, tal como TLS v1.2, para proteger los datos de sus clientes.

Más información: Suplementos informativos sobre el uso de SSL/TLS inicial

CONSEJO NO. 5: USE ACCESO REMOTO SEGURO

Para reducir al máximo el riesgo de que se produzcan filtraciones, es importante que usted participe en administrar cómo y cuando pueden acceder sus proveedores a sus sistemas. Los delincuentes pueden obtener acceso a sistemas que almacenen, procesan o transmiten datos de pagos a través de controles de acceso remoto no seguros. Le recomendamos limitar el uso de acceso remoto y deshabilitarlo cuando no sea necesario. Si debe permitir acceso remoto, pida a sus proveedores que utilicen autenticación multifactor y credenciales de acceso remoto seguras que sean únicas para su empresa y no las mismas que usan otros clientes.

Más información: Infografía de PCI SSC sobre acceso remoto seguro

CONSEJO NO. 6: ASEGÚRESE DE QUE LOS FIREWALLS SE CONFIGUREN CORRECTAMENTE

Un firewall es un dispositivo o software que se sitúa entre su red y la internet. Actúa como una barrera para evitar el tráfico que no desea y no autorizó en sus redes y sistemas. Las reglas de los firewalls pueden parecer complejas, pero configurarlos adecuadamente es vital para la seguridad. Si requiere ayuda para configurar su firewall correctamente, consulte a un profesional en redes.

Más información: Recurso para pequeños comerciantes: Conceptos básicos sobre firewalls

CONSEJO NO. 7: PIENSE ANTES DE HACER CLICK

Los hackers usan phishing y otros métodos de ingeniería social para dirigirse a empresas con correos electrónicos y mensajes de redes sociales que parecen legítimos, para lograr que los usuarios engañados proporcionen datos confidenciales, tales como número de tarjeta de pago, número de cuenta o contraseña del comerciante. Los pequeños comerciantes deben estar extremadamente atentos y alertas a los trucos comunes de phishing e ingeniería social.

Más información: Cuidado con las estafas y amenazas en línea relacionadas con el COVID-19

CONSEJO NO. 8: ELIJA SOCIOS DE CONFIANZA

Es fundamental que sepa quiénes son sus proveedores de servicios y qué preguntas de seguridad debe hacerles. ¿Su proveedor de servicios se apega a los requisitos de PCI DSS? En el caso de comerciantes de comercio electrónico (y aquellos que recientemente empezaron a aceptar pagos de comercio electrónico en lugar de cara a cara), es importante que sus proveedores de servicios de pago cumplan con PCI DSS, incluido el proveedor de servicios que administra su proceso de pagos (su "proveedor de servicios de pago" o PSP).

Más información: Preguntas que debe hacer a sus proveedores

MATERIALES COMPLEMENTARIOS DE FONDO DE PCI SSC

Mejores prácticas para proteger el comercio electrónico

Protección de los datos de tarjetas en pagos por teléfono

Protección de los pagos al trabajar de manera remota

Guía para realizar pagos seguros

Preguntas que debe hacer a sus proveedores

Sistemas de pago comunes

El Consejo ha establecido recursos para actualizar la información acerca del COVID-19; lo invitamos a echar un vistazo a nuestra página web sobre COVID-19 y nuestro blog con regularidad, ya que estamos ante una situación en constante evolución.

También puede suscribirse a nuestro blog para recibir alertas por correo electrónico.