3 PASOS PARA PROTEGER A TU NEGOCIO

de los ataques de prueba de tarjeta.

CyberSource®
A Visa Solution

La prueba de tarjeta sucede cuando un atacante «prueba» un número de tarjeta que probablemente ha comprado en la web oscura, o que ha obtenido vía phishing o software de programas espía. El objetivo principal de las pruebas no es la compra de un producto o servicio, sino verificar si los detalles de la tarjeta son válidos intentando pequeñas compras online en el sitio de un comercio desprevenido y luego verificando la respuesta para ver si la tarjeta fue aprobada.[1]

1

Asegúrate que las páginas de checkout incluyan tecnologías para la detección y prevención de envío de transacciones desde scripts automatizados como:

a. **Firewalls.** Herramientas para la detección, prevención y eliminación de botnets.
b. **CAPTCHA.** Una prueba visual de tipo desafío-respuesta para distinguir a un humano de un script automatizado.
c. **Identificación de huellas digitales** Identifica múltiples contactos desde el mismo dispositivo.
d. **Umbrales de velocity.** Limitan la cantidad de transacciones permitidas en un período de tiempo.
e. **Detección de anomalías.** Detección de picos inusuales en el tráfico de una página web, patrones inusuales durante la compra o en el llenado de formularios.

2

Si el sitio acepta donaciones o montos de pago de texto libre, es importante que incluya medidas para evitar scripts automáticos y pruebas de tarjeta. Estos sitios son vulnerables. Además de los pasos anteriores, ten en cuenta lo siguiente:

Establece montos mínimos elevados. El defraudador utiliza montos muy pequeños, a veces iguales a cero, para no llamar la atención y poder confirmar la validez de la tarjeta sin que el titular lo note y lo reporte. Establece un monto mínimo elevado, adecuado para tu negocio, para que esto no suceda.

3

Manténte alerta e identifica cualquier anomalía con antelación.

a. **Investiga** cualquier cambio en transacciones diarias.
b. **Atención** a los aumentos repentinos en la cantidad de rechazos de tarjetas.
c. **Utiliza herramientas** de velocity para hacer un seguimiento de los totales y otros datos específicos.

Algunas herramientas que pueden ayudar en la prevención de ataques de prueba de tarjetas:

Account Takeover Protection (ATP) de CyberSource
Para comercios que ofrecen abrir nuevas cuentas online.

Device Fingerprinting
Identifica bots y tecnología para atravesar servidores proxy.

Implementación de pruebas para detectar fraude
Durante la creación de cuentas e inicios de sesión.

Reglas de Velocity desde Decision Manager (DM)
Seguimiento, conteo y rechazo de intentos repetidos.

Límites de montos establecidos
Limita transacciones solamente a las que sean adecuadas a tu negocio.

CyberSource protege a tu negocio de los ataques de prueba de tarjeta.

Si desea conocer más sobre cómo CyberSource puede ayudarlo, contacte a su equipo de administración de cuenta de CyberSource o visite www.cybersource.com

CyberSource® | A Visa Solution

[1] The Ever-Changing Landscape of Bots and Credit Card Testing, by John Canfield, April 26, 2018, business.com: https://www.business.com/articles/bots-credit-card-testing.