



## PASOS PARA PROTEGER A TU NEGOCIO

de los ataques de prueba de tarjeta.



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.<sup>1</sup>



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.



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.



Mantente 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](http://www.cybersource.com)

<sup>1</sup> 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>.

#### Limitación de Responsabilidad

La información, recomendaciones o "mejores prácticas" contenidas en el presente documento se proporcionan "tal cual están", son a mero título informativo y no deberán considerarse como asesoría de negocios, operativa, comercial, financiera, legal, técnica, fiscal o de otro tipo. Los costos, ahorros y beneficios reales de toda recomendación, programa o "mejor práctica" variarán dependiendo de sus necesidades comerciales y requisitos de programas específicos. Por su naturaleza, las recomendaciones no representan garantía de desempeño o resultados futuros y están sujetas a riesgos, incertidumbre y presunciones difíciles de predecir o cuantificar. Nuestras presunciones se hicieron a la luz de nuestra experiencia y percepción de tendencias históricas, condiciones actuales, desarrollos futuros esperados y demás factores que consideramos apropiados según las circunstancias. CyberSource no es responsable por el uso que usted haga de la información contenida en el presente documento (incluidos errores, omisiones, imprecisiones o falta de oportunidad de cualquier tipo), ni de presunción o conclusión alguna que usted pudiere inferir de su uso. CyberSource no otorga garantía alguna, expresa o implícita, y expresamente renuncia a las garantías de comerciabilidad e idoneidad de uso para un propósito en particular, a toda garantía de no violación de los derechos de propiedad intelectual por parte de un tercero, a toda garantía de cumplimiento de la información con los requisitos de un cliente o a toda garantía de actualización de la información y de información sin errores.