3 PASSOS PARA PROTEGER SEU NEGÓCIO

contra ataques de teste de cartão.

CyberSource®
A Visa Solution

O teste de cartão acontece quando um criminoso "testa" um número de cartão de crédito comprado na dark web ou obtido por meio de phishing ou spyware. O objetivo principal do teste não é comprar um produto ou serviço, mas verificar se os detalhes do cartão são válidos. Para isso, o criminoso tenta fazer pequenas compras online no site de um estabelecimento comercial desavisado para ver se o cartão é aprovado.[1]

1

Proteja suas páginas de checkout com tecnologias que detectam e evitam que scripts automatizados enviem transações:

a. **Firewalls.** Ferramentas de detecção, prevenção e eliminação de botnets.
b. **CAPTCHA.** Desafio visual usado para distinguir usuários reais de scripts automatizados.
c. **Identificação de impressão digital.** Identifica múltiplos contatos de um mesmo dispositivo.
d. **Limites de tentativas.** Limita o número de transações permitidas dentro de um período específico.
e. **Detecção de anomalias.** Detecção de picos repentinos ou incomuns no tráfego de sua página web, bem como padrões incomuns de compras ou de preenchimento de formulários.

2

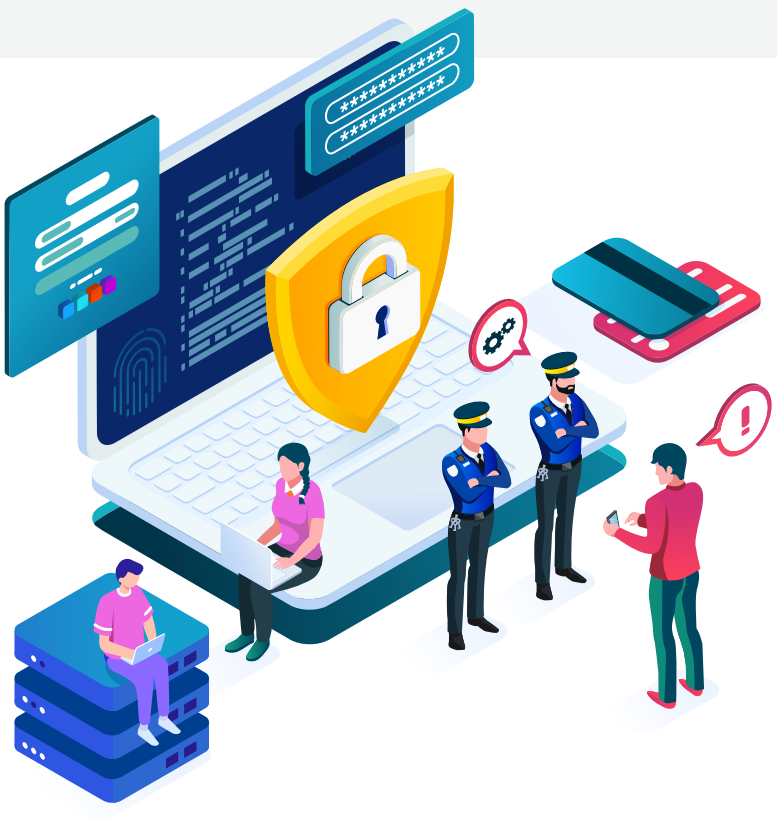
Se o seu site aceita doações ou montantes de pagamento de texto livre, é importante incluir medidas para prevenir o uso de scripts automatizados e testes de cartão, pois esses sites são mais vulneráveis. Além dos passos anteriores, outras melhores práticas são:

Estabeleça montantes mínimos elevados. O fraudador utiliza valores baixos, muitas vezes iguais a zero, para não chamar atenção e poder confirmar se o cartão está válido, sem que o titular do cartão note e reporte a fraude. Estabeleça um montante mínimo elevado, mas ainda adequado à realidade do seu negócio, para que isso não aconteça.

3

Fique atento e identifique anomalias logo no início.

a. **Investigue** qualquer aumento repentino e inesperado nas transações diárias.
b. **Atenção** aos aumentos súbitos no número de cartões de crédito recusados.
c. **Use ferramentas** de controle de tentativas para monitorar os totais das transações e outros dados específicos.



Ferramentas que podem ajudar na prevenção de ataques de testes de cartão:

CyberSource Account Takeover Protection (ATP)
Para estabelecimentos comerciais que permitem a criação de novas contas online.

Impressão digital de dispositivos (Device Fingerprinting)
Identifica bots e tecnologias para atravessar servidores proxy.

Implementação de métodos de detecção de fraude
Durante a criação de contas e inícios de sessão.

Regras de velocity do Decision Manager (DM)
Monitoram, contam e rejeitam tentativas de transação repetidas

Definição de limites de montantes
Limitam as transações aos montantes apropriados ao negócio.

A CyberSource protege seu negócio contra ataques de teste de cartão.

Para saber mais como a CyberSource pode ajudar, contate a equipe de vendas da CyberSource ou acesse 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.