



PASSOS PARA PROTEGER SEU NEGÓCIO

contra ataques de teste de cartão.



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



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.



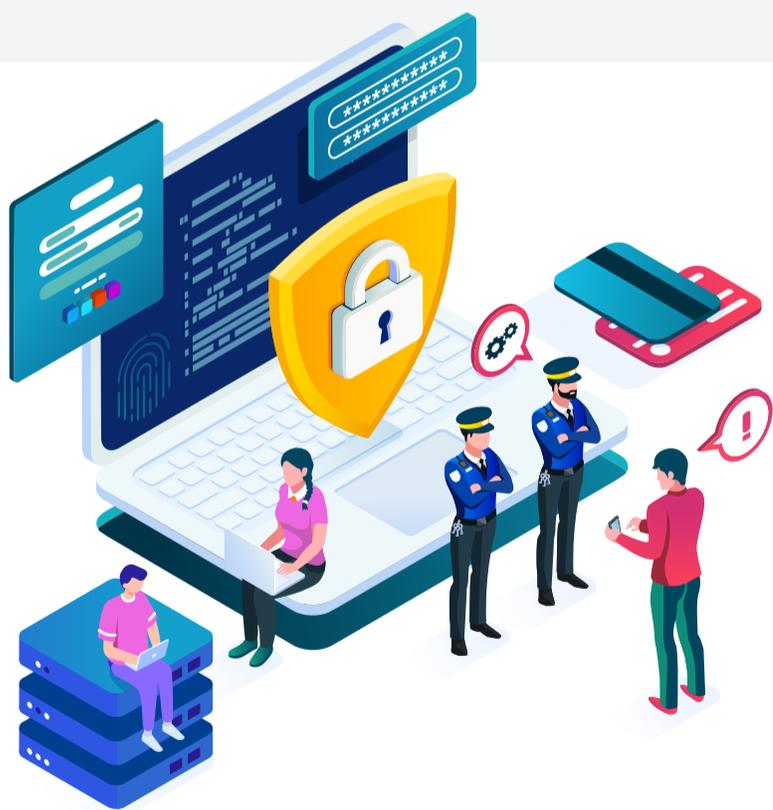
Se o seu site aceita doações ou montantes de pagamento de texto livre, é importante incluir medidas para prevenir o uso de scripts automatizados e testes de cartão, pois esses sites são mais vulneráveis. Além dos passos anteriores, outras melhores práticas são:

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.



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

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>.

Limitação de Responsabilidade

As informações, recomendações ou “melhores práticas” aqui contidas são fornecidas “no estado em que se encontram”, a título meramente informativo e, assim, não devem ser consideradas como uma assessoria de negócio, operacional, de marketing, financeira, jurídica, técnica, fiscal ou de qualquer outro tipo. Os custos reais, economias e benefícios resultantes de referidas recomendações, programas ou “melhores práticas” podem variar com base em suas necessidades específicas negociais e nos requisitos do programa. Pela sua natureza, as recomendações não são garantias de desempenho futuro ou resultados e estão sujeitas a riscos, incertezas e suposições que são difíceis de prever ou quantificar. Suposições foram feitas por nós à luz da nossa experiência e nossas percepções de tendências históricas, das condições atuais e dos desenvolvimentos futuros esperados e outros fatores que acreditamos sejam adequados sob a circunstância. A CyberSource não é responsável pelo uso que você faça da informação aqui contida (incluindo erros, omissões, imprecisões ou faltas de oportunidades de qualquer tipo) ou por quaisquer suposições ou conclusões que você possa tirar do seu uso. A CyberSource não oferece nenhuma garantia, expressa ou implícita e renuncia explicitamente as garantias de comercialização e adequação a uma finalidade específica, a toda e qualquer garantia de não violação de direitos de propriedade intelectual de qualquer terceiro, qualquer garantia de que a informação irá atender aos requisitos de um cliente ou qualquer garantia de que a informação é atualizada e será livre de erros.