e-commercebrasil
EXCELÊNCIA EM E-COMMERCE

Oferecimento: CERTISIGN SITE BLINDADO

pocket Segurança e Anti Fraude

Guia de estudos sobre Segurança e Anti Fraude

Produzido entre 07 a 18 de maio de 2012, pelo Projeto E-commerce Brasil

Mais informações em: http://www.ecommercebrasil.com.br/

Atualmente se pode abrir uma loja virtual pagando R$30,00 por mês e em 5 minutos prometem uma loja funcional rodando com meios de pagamento e logística já integrados. Isso fez explodir no Brasil o número de lojas virtuais pequenas e algumas delas hoje são lojas medianas, que em geral são marcas conhecidas em uma região que acabam atingindo o estado inteiro onde elas estão inseridas.

As fraudes no mundo, segundo uma pesquisa da CyberSource (EUA), estão em torno de US$ 10 bilhões ao ano e, no Brasil, representam aproximadamente US$ 500 milhões.

Os comerciantes no mundo real já lidam com fraudes no seu dia a dia, tais como cheques e cartões de crédito roubados, cheques sem fundo etc. No caso do comércio virtual, há esses riscos e alguns outros, devido ao fato de não haver certezas com relação à identidade do comprador e à veracidade das informações fornecidas. Esse é o tipo de fraude mais comum, ou seja, a compra de um bem ou serviço, através de um meio de pagamento fraudulento, principalmente os cartões de crédito.

Qual é o caminho, então? Perder a venda? O vendedor deverá considerar o risco como parte do negócio, ou seja, não há negócios sem risco. Sendo assim, ao ter consciência disso, ele deverá medir qual é o provável índice de perda e verificar a possibilidade de incluir esse percentual no seu custo. Por outro lado, obviamente, deverá lançar mão de estratégias que reduzam esse risco e suas perdas.

Durante o workshop - **Aspectos Técnicos de Segurança para e-commerce,** aplicado pela Maria Teresa Aarão, Gerente de Desenvolvimento de Novos Produtos da Certisign Certificadora Digital foram relembrados:

1 - Mantra da segurança no e-commerce:

a) Identificação: quem está falando

b) Autenticação: como provou que é quem diz ser?

c) Autorização: o que este interlocutor pode fazer?

d) Confidencialidade: como garantir o sigilo?

e) Integridade: tem proteção contra modificação indevida?

f) Não repúdio: tem uma estratégia de recuperação?

g) Auditoria/responsabilidade: é passível de verificação por terceiros? Todas as ações tem autoria identificável?

2 - Seis objetivos e os 12 requisitos do PCI DSS

a) Construir e manter uma rede segura

- Firewal para proteger os dados dos clientes

- Não usar as configurações e senhas padrão dos fabricantes

b) Proteção dos dados do cliente

- Proteger dados de clientes armazenados em seus bancos de dados

- Criptografar dados de clientes para transmissão em rede aberta

c) Manter um programa de gerenciamento de vulnerabilidade

- Usar e atualizar regularmente programas anti-virus

- Desenvolver e manter sistemas e aplicações seguras.

d) Implantar medidas de controle de acesso forte

- Restringir o acesso aos dados pela necessidade de saber do negócio

- Designar uma identidade única para cada pessoa com acesso ao computador que guarda os dados

- Restringir o acesso físico aos dados dos clientes

e) Monitorar e testar sua rede regularmente

- Rastreie e monitore todos os acessos a dados de clientes

- Testar regularmente a segurança de sistemas e processos

f) Manter uma política de segurança de informação

- Construa uma política de segurança da informação que aponte ações para todos os funcionários.

Alguns números apresentados durante o workshop - *(Fonte:Zooknic, Verisign, ICANN - outubro 2011):*

- O terceiro trimestre de 2011 foi encerrado com uma base de quase 220 milhões de registros de nomes de domínios em todos os Domínios de Primeiro Nível (TLDs).

- Os registros aumentaram mais de 18 milhões, ou 8,9% desde o terceiro trimestre de 2010.

- Novos registros *.com* e *.net* atingiram um total de 7,9 milhões no trimestre. Isto indica um aumento ano a ano de 5,9% de novos registros, e uma queda de 2,3% sobre o segundo trimestre.

- Dentre os 20 maiores ccTLDs, Brasil, Austrália, Tokelau e Federação Russa ultrapassaram um crescimento trimestre a trimestre de 4%.

- A taxa de renovação de .com e .net no terceiro trimestre de 2011 foi de 73,3% um

aumento sobre 73,1% do segundo trimestre. A taxa de renovação varia no trimestre de acordo com a composição da base de nomes para expirar e a contribuição de registradores específicos.

De acordo com dados de mercado, aconteceram mais de 3,1 bilhões de ataques através de malware na web durante 2010. E, pela segunda vez consecutiva, o Brasil foi o país com maior número de casos da América Latina, com 8% desse montante. Além disso, o país também é o quarto maior desenvolvedor de softwares maliciosos do mundo, sendo berço de 4% das ameaças.

Fraude

Um dos maiores obstáculos às vendas virtuais é a fraude. A explicação é simples: ao contrário das vendas presenciais, nas quais o lojista tem a possibilidade de solicitar prontamente a assinatura, as senhas e os documentos que comprovem a identidade do cliente, em compras não-presenciais torna-se difícil saber se quem está efetuando a compra é de fato o portador do cartão.

É, assim, fundamental conferir se quem está realizando a compra é o real portador do cartão de crédito. Em outras palavras, é preciso perguntar “você é você?”, de maneira não-invasiva, prática e assertiva a cada transação de venda. Deve-se, também, evitar requerer documentos e adicionar passos desnecessários ao e-commerce, uma vez que processos burocráticos tendem a abrir espaço para cancelamentos.

Durante o curso de **Formação em Análise e gestão de risco de fraude**, aplicado pela Arlene Affonso, responsável pelas Relações Institucionais da ClearSale foram apresentados o tipos de estorno (chargeback) que temos no e-commerce:

- Fraude deliberada = o verdadeiro dono do cartão não fez a compra

- Auto-fraude = verdadeiro dono fez a compra e dissimula (má fé)

- Fraude amigável = pessoas próximas do verdadeiro dono fizeram a compra (não existe má fé)

- Desacordo comercial = todas as outras situações.

Avaliação de Fraude	Avaliação de Crédito
Falsidade DO ser	Falsidade DE ter
Autenticar comprador - É ele?	Validar crédito - Pode pagar?
Dados cadastrais	Restrições de crédito
Não reconhecimento	Não pagamento
Fraude	Inadimplência
Positivar os dados	Retirar restrições creditícia

O que é importante observar para predizer a falsidade ideológica?

- Histórico positivo compartilhamento

- Base de alertas (com positivação)

- Geolocalização do IP

- Finger Print - device ID

- Batimento cadastral

- Correto tratamento dos riscos globais

- Perfil do pedido

Consequências da fraude virtual

Não impedir a falsidade ideológica no meio virtual acarreta prejuízos enormes ao

lojista, pois, caso não reconheça a compra, o real portador do cartão poderá solicitar o cancelamento da compra, gerando o estorno – também conhecido por chargeback.

Ao contrário do que se pensa, a responsabilidade pelo chargeback não é da administradora do cartão, que apenas verifica a existência de saldo, mas do lojista. Assim, para evitar prejuízos desnecessários ao seu negócio, cabe prevenir-se com ferramentas que combatam ações fraudulentas, sem cancelar bons pedidos por excesso de zelo.

“Não me preocupo com isso, pois não tenho fraudes!”

Não se deparar com a fraude não indica, necessariamente, estar negociando de maneira inteligente. Muitos acreditam que, com fornecedores adequados, é fácil manter a fraude sob controle, mas não ter fraudes pode significar vender menos.

Lojas com baixos índices de fraude tendem a apresentar um número maior de cancelamentos. Cerca de 90% da lucratividade corresponde a um aumento nas vendas, o que comprova que tão importante quanto monitorar o índice de fraudes é verificar o índice de cancelamentos.

Além disso, a reprovação de um bom cliente não é somente a perda de uma venda, é a perda de um (ou muitos) cliente(s), pois o ele repassa, no seu círculo social, a impressão obtida durante o processo de compra e, caso tenha ficado insatisfeito, a má impressão poderá ser propagada em efeito dominó. Por outro lado, se o cliente vivenciar uma experiência que atenda às expectativas, a tendência é que ele se fidelize a sua loja, recomendando-a a outras pessoas.

Assim, o que importa, de fato, é o resultado final da operação, que deve estar guiado por um bom balanceamento entre a quantidade de pedidos, o custo gerado e o risco de perda, que varia de acordo com a exposição de sua loja.

No processo de combate à fraude, é fundamental a valorização do bom pedido. O histórico da ClearSale indica que apenas 3% das vendas são tentativas de fraude, o

que potencializa a importância em atender os 97% restantes com rapidez e assegurar o sucesso das vendas legítimas em vez de canalizar o foco exclusivamente à detecção de fraudes. Enfatizando-se a ideia de que “a maioria é boa!” e, ao tratar o cliente legítimo com prioridade, consolida-se um vínculo de cumplicidade entre o consumidor e o vendedor.

Com o aumento da profissionalização do e-commerce no País, podemos observar que o cenário tem melhorado e apresentado cada vez mais segurança para todos os participantes do processo de compras.

GUIA DE ESTUDOS

1) Token no e-commerce: eis a questão

2) Como decidir o melhor modelo de gestão de riscos para o seu e-commerce

3) Segurança virtual não é mais diferencial, é obrigação

4) PPT - Workshop: Aspectos técnicos de segurança para e-commerce

5) PPT - Webinar: Os 10 erros mais comuns de segurança na operação de um e-commerce.