



Tips For Safe Holiday E-Commerce

[Home](#) > [E-Commerce](#) > [Tips For Safe Holiday E-Commerce](#)

Author:

By Sandeep Walia

Publishing date: Dec 18, 2006 07:20

Online shopping has hit high gear—and so have thieves' efforts to compromise systems and steal money. These four tips are designed to ensure that your New Year is a happy one.

TIPS FOR SAFE HOLIDAY E-COMMERCE

This holiday season, Forrester Research expects a 23 percent rise in online sales, to \$27 billion total. Cyber Monday, which marks the first spike in online spending after Thanksgiving, saw higher than expected gains with sales of \$608 million, which is up 26 percent from last year.

With the holiday shopping season upon us, e-tailers are on high alert with credit card fraudsters looking to cash in. Smaller businesses are most at risk as they are often considered easier prey for credit card fraud in comparison to larger online storefronts with more IT resources. But it is not uncommon for even larger e-tailers to fall prey.

According to a recent report by Gartner Group, \$2 billion in e-commerce sales have been lost in 2006 because of security fears. The firm estimates that half of those losses came from consumers avoiding sites that appeared to be less secure, while the remainder came from those refusing to buy online at all due to security concerns.

Ignify specializes in e-commerce and ERP solutions for the mid-market and enterprise business segments. We find that companies do not often get serious about security until they are hit with serious fraud.

Before approaching Ignify, US Digital Media, a leading supplier of optical digital media, recently lost upwards of \$200,000 due to credit card scams even though necessary network security precautions were in place. In one instance, the company was targeted (because of its merchandise) by a sophisticated team of criminals involved in a larger international movie pirating operation.

Although fraud prevention was a key area of concern for US Digital Media, another major area was the ordering cycle. It took up to five hours to get product out the door because of the lack of integration with the ERP, accounting and shipping systems, costing the company tremendously in lost revenue.

US Digital Media chose to deploy the Ignify eCommerce platform. Ignify's special heuristic screening method brought credit card fraud loss down to non-existent levels. Over time, the system actually learns customer buying patterns.

In addition to security improvements, US Digital Media's ordering cycle was also reduced to minutes instead of hours since the Ignify platform integrated into back office operations making order processing fully automated.

Ignify, a Microsoft Gold Certified Partner with offices in Los Angeles, Silicon Valley, Nashville, Toronto, and India, offers SmartBiz readers a few simple tips for improving e-commerce security for little or no investment.

Even senior IT professionals should review these tips. While they may know some of the suggested precautions, there is a high likelihood that they may not know that their organization doesn't follow them. It is not uncommon for even IT departments to be unaware of the details of an implementation.

E-Commerce Security Tips

Make sure you have an Address Verification System (AVS), which will run automatically when the order is placed. AVS matches the customer's credit card number with his or her billing zip code. The AVS can be set at a higher level to

match the credit card with the customer's complete billing address, but companies can run the risk of getting many false positives with this higher setting.

Screen orders that meet certain criteria for an additional level of verification and follow this process consistently every day. For example, screen all orders over \$200 going to a PO Box or scheduled for overnight delivery, so the order may be put on hold and reviewed before processed.

The trick to fraud is managing by exception. Most merchants add more people instead of improving their systems. Let the system catch the exception instead of trying to eyeball each order.

Pre-authorize credit cards automatically when the order is placed. Setup systems to charge the card automatically when the order is shipped out. Don't store credit card numbers, just store authorization codes to protect your business from any kind of security breach such as a server hack.

Ensure that your fraud prevention is not limited to credit card orders. Bogus checks and Western Union transfers also have a high incidence of fraud. It may be prudent to put database encryption in place as well.

If you don't have time to build something fancy - you could reduce fraud by simply running a fraud check report on select parameters two or three times a day. This will help to red-flag orders that are suspect. Even something as basic as this could cut your fraud by 50 percent.

Email This Story

Receiver's email:

Your email:

Send Article

* Both fields are required

| [Back to normal page view](#) | [Email Article](#) |
