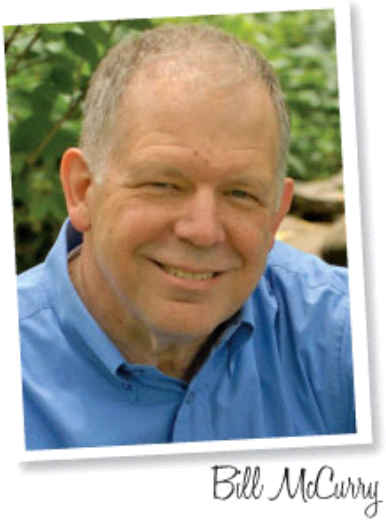
greenPROFIT

Columns

8/31/2017

Online or Off?

Bill McCurry



The sky is falling! Retail is dead! Only Amazon will survive! Independents are doomed!

Enough already!

Take a deep breath. Evaluate your strengths and your weaknesses. Capitalize on your strengths and shore up your weaknesses so they aren't fatal. This doesn't mean run headlong into massive web investment with no awareness of the reality of today's world.

Both mass and social media are forecasting retailer doom and gloom, claiming online is the only solution. Yes, while online is grabbing a growing share of discretionary dollars, throwing half your current ad budget into building an "improved" website may not be your answer. It may be creating a new problem: Online fraud or security issues.

Recently, I enjoyed a conversation with Stirling McBride, director of Fraud Investigation for Microsoft. Stirling isn't an official spokesperson for Microsoft. He's a great human being who has extensive experience attempting to protect against cybercrime. Stirling and I discussed a few common-sense observations that can help you understand some of the online risks.

• If you have an e-commerce presence, it's not if you'll get defrauded, it's how bad it will be. "As we see with each new computer virus attack, many small businesses don't do the routine updates and that leaves them vulnerable," Stirling says. "Business owners know the right thing to do, but they claim they don't have the time to do it. Then when the crises do hit, they find the time to spend hours/days rebuilding their systems, suffering massive overtime costs to restore their systems, loss of sales and immense frustrations."

• "Storing customer data attracts hackers. Most consumers use similar passwords on multiple sites, which increases their value to identity thieves. If you require user passwords, hackers will find that fertile ground. Consider why your customers need passwords for your site. Don't store data that invites fraudsters," he says.

• “As a merchant you must respect the Payment Card Industry Data Security Standard (PCI DSS),” Stirling notes. “Outsource your credit card processing and data storage to professionals with advanced security apparatus. Consider secure cloud storage for all your storage needs.”

• If you believe you have a future in e-commerce beyond your local market area, consider your website from a newcomer’s perspective. If they don’t know you, do you look credible? Are there reviews or testimonials reassuring first-time visitors? If first-timers are hesitant, can they use Pay Pal rather than submitting their credit card information?

• “Use trade groups, buying groups and similar events to discuss common security risks with your peers,” Stirling says. “The bad guys share information about which companies are easy targets and how to overcome the latest security updates. Merchants need to have similar communication channels.”

“Friendly fraud” is an oxymoron. It refers to the “customer” who orders online and is intent on ripping you off. The most common way to do this is to claim the order wasn’t delivered. The carrier reports they left it on the front porch. The customer claims it never got there. Amazon spoiled online customers by instantly replacing these “non-delivered” packages—feeding the fraud. While Amazon doesn’t share their anti-theft policies, we hear anecdotally if an address/account has frequent “non-deliveries,” Amazon no longer sends a replacement until the customer provides the police report number with the reporting officer’s badge number. A different scam involves asking UPS to change the delivery address to one that doesn’t match the credit card company’s address of record. The retailer eats the loss.

If you believe you have effective offerings for e-commerce, please maximize your assets and make it happen. But recognize it’s not all easy money. There are people online who want your money more than you do. It’s up to you to protect yourself—before you launch your new e-commerce venture! **GP**

Bill would love to hear from you with questions, comments or ideas for future columns. Please contact him at wmccurry@mccurryassoc.com or (609) 688-1169.