

BRANDWEEK®

JUNE 12, 2009

MarkMonitor CEO on Brand Fraud, Risks Brands Face Online



As commerce and marketing efforts continue to shift online, brands' exposure to risks are increasing, according to Irfan Salim, CEO of MarkMonitor, a firm specializing in enterprise brand protection. In a recent

Q&A with Nielsen Business Media's managing editor Kenneth Hein, Salim discussed the risks brands face online and the tactics they can adopt to protect themselves. Excerpts of that conversation are below:

Nielsen Business Media: What are the current trends in brand fraud?

Irfan Salim: Online attacks are reflections of what has been happening in the physical world since day one. However, the unique brand risk online is that these attacks have a significant multiplier effect. In the physical world, your sphere of influence may be the street corner, dude, but online – every criminal has a global market.

Think about the effect on your brand when this multiplier effect is applied. Explosive availability of fake products and grey market goods in e-commerce channels. Junk mail a problem? Spam is online junk mail on steroids. Phishing and malware attacks that exploit your brand are akin to a globally mobilized virtual dumpster diving squad.

Whatever problems your brand faces in the physical world, in the online world, multiply those problems by thousands of instances and then multiply the result by ten times the sophistication. I think of it as the five A's: Any company, Any product can be targeted Anywhere and Anytime by someone Anonymous.

NBM: How have the tactics shifted?

IS: There's a constant cat and mouse battle with brandjackers and brands. However, in the last year, we're seeing the scammers concentrate increasingly on weak spots in Internet

infrastructure in order to hide their tracks – ISPs (Internet Service Providers), domain registries, even registrars. For example, last year a nest of scammers targeting the pharmaceutical sector was identified operating out of a domain registrar in Estonia, whose CEO was a convicted criminal. That business was shut down but we continue to see sophisticated criminal groups joining the ranks of brandjackers.

These scams create real problems for marketers especially for those who are trying to accelerate the adoption of e-commerce, online banking or other e-business initiatives.

NBM: Give me an example of one brand that was affected?

IS: The pharmaceutical example I just mentioned is chilling due to the potential for damage to human life, in addition to a brand's reputation. In March of 2007, a Canadian woman died after taking counterfeit name-brand drugs that she bought on the Internet.

You have to realize that the scammers and criminals who play this trade are creative and quick to take advantage of the public's concerns. For example, we did a scan recently over a period of a few days and discovered more than 50 online pharmacies selling Tamiflu; only two of those pharmacies were properly accredited. Five of the pharmacies had been set up within a week of the first CDC news conference on the swine flu pandemic and each of those five used the brand name Tamiflu in their domain name.

NBM: Are brands being attacked via social media?

IS: There's a multi-pronged thrust in this regard. The social media platforms themselves are being attacked because their role as communications platforms is seen by scammers as an easy way to spread nasty code. The goal is to infect the accounts of social media users to steal credentials as well as to continue

spreading nasty code by exploiting trusted connections. Get the password/user name combo on a social media site and the scammer may have the keys to multiple accounts for that individual including financial accounts or business accounts for other brands. Why? People often use the same password across different sites and scammers understand human nature.

And, of course, every good marketer knows the importance of tracking user sentiment on social media sites. That feedback can be very useful in building the business case for new products or services, or in improving brand loyalty.

NBM: What sector is the most vulnerable?

IS: No sector is immune. If your brand is well known, it is a target. We started publishing a Brandjacking Index in 2007 to examine how leading Interbrand-ranked brands are abused online. We have found significant growth in online abuses in every sector – apparel, luxury, financial, high tech, automotive, pharmaceutical, consumer goods, you name it.

The most common abuses are based on cybersquatting, in which scammers abuse well-known brands in domain names. The idea is to divert traffic, manipulate SEO results, conduct illicit e-commerce or take advantage of pay-per-click advertising.

Furthermore, it's very important to note that if your pricing strategy depends on perceived brand value, then your products are especially at risk for counterfeiting. The Internet gives counterfeiters a global market.

NBM: What is the one thing that most brand managers aren't even thinking about that they should be?

IS: Brand managers spend billions in advertising and other promotional programs to build their brand assets yet brand managers pay little to no attention to how those assets are seeping out of their control online.

MarkMonitor®