

## in this issue

1

Microsoft Readies  
'A1' Security  
Subscription Service

2

Bar-Code Scam at  
Wal-Mart: A Matter of  
Priorities

3

Search Engine Spam?  
You're Fired!

•

Microsoft Cans  
Windows 2000 SP5

4

Will Branded  
Keywords Kill Search?

•

Accountant's  
Tips

February 2005 - Vol. 02-05

## Microsoft Readies 'A1' Security Subscription Service

**Microsoft's anti-virus/anti-spyware strategy is taking shape. Sources say Redmond's prepping a fee-based bundle, which could go beta soon.**

Publicly, Microsoft continues to be cagey about packaging and pricing plans for its anti-spyware and anti-virus solutions. But privately, Microsoft has begun informing partners of its plans for a security subscription service code-named "A1," according to developers who requested anonymity.

Microsoft bought anti-virus vendor GeCAD in the summer of 2003, and anti-spyware maker Giant Company Software last month. As to how it plans to deliver these technologies, Microsoft has declined to give specifics. How/when/if it will repackage GeCAD's technology remains uncertain.

The Giant Software has been repackaged as a Beta version called "Microsoft Anti-Spyware" and was released last week as a freetrial with a time limitation of 200 days.

Microsoft officials have said the company is planning to make some form of its anti-spyware product available as a free tool. But that isn't the ultimate plan, partner sources said.

Microsoft is currently expecting to field its A1 anti-spyware/anti-virus bundle in the form of a renewable subscription service, the same way

a number of other security vendors do, sources said. The service will allow users to keep current on the code needed to combat ever-changing viruses, worms, spybots and the like.

Some elements of A1 are likely to be built directly into future versions of Windows, according to partners. Specifically, some of the security-management functionality, such as the security-health-validation technology which Microsoft officials discussed last year, would likely be bundled into Windows itself, partners said.

The degree to which A1 will draw from learnings from Microsoft's "PC Satisfaction Trial," which the company conducted between 2003 and early 2004, is uncertain. PC Sat was designed to test Microsoft and third-party anti-virus, firewall, backup and PC-health-monitoring services. Sources said that Microsoft was testing whether these kinds of security services — when provided as hosted, managed services — would appeal to typically less-security-savvy small-business and consumer customers. Microsoft officials have declined to comment on the trial.

Microsoft officials also declined to comment on A1. Amy Carroll, director of Microsoft's security business and technology unit said: "We have not finalized the productization plans, and beyond that, we can't talk about the company's future anti-spyware/anti-virus solutions."

# Microsoft®

isi

18530 Spring Creek Drive - Tinley Park, IL 60477

tel: 708.532.8488 - fax 708.532.8493

www.intelligentsolutions.net

# Bar-Code Scam at Wal-Mart: A Matter of Priorities

In a recent bar-code scam against Wal-Mart and others, thieves went through considerable trouble in scanning in low-priced bar codes, printing out duplicates and then surreptitiously placing them over the correct bar codes on higher-priced items.

“I really wasn’t surprised,” says Chris Dorsey, CIO at the Chase-Pitkin chain of home and garden supplies. “There have been people who have duplicated receipts. [It’s possible] with the right printers, the right copiers in place.

“And there’s an old game called sticker-swapping, where [the thief] goes into a store and looks for packages where they can easily peel off the old sticker and put it on a different product. This is just the next evolution of sticker swapping.”

To foil the plot, all that had to happen was for one cashier at any of the hundreds of victim stores—in any one of the 19 states targeted—to have looked up and seen that the item on the screen was clearly not the item in front of them.

Suffice it to say, it never happened. Not once. It was like a retail version of “A Streetcar Named Desire.” This version, “A Shopping Cart Named Desire,” features shoplifter Blanche DuBois declaring, “I’ve always relied on the apathy of strangers.”

Apathy is just about right. Some might jump to the reaction that it’s something much harsher, such as incompetence or stupidity. But it wasn’t. The cashiers here were—for the most part—following their instructions, which is typically to move the line along as quickly as possible.

If a cashier opts to be careful and check items visually against what the screen reports (assuming they are even looking at the screen for every item, which is a really unlikely assumption), they’ll get dinged for slowing down the line.

And what happens when a bandit does slip something by them? For most retailers, if the cashier was not a knowing accomplice and did not profit from the theft (in other words, if the cashier was duped and had no criminal intent), the cashier is not disciplined. Therefore, what incentives are put in place? A huge incentive to keep the

line moving, and almost none to slow it down and be more careful.

The evitable question prompted by a case such as this is, “If thieves can replicate today’s bar codes, can’t we make bar codes that are much more difficult to replicate?” From a technology standpoint, the answer is “absolutely.”

Many such devices exist today—such as 2-D barcodes, covert ink and product-level RFID chips—but this gets back to the ROI question. How much more can a retailer justify spending on a low-priced—and razor-thin-margined—item?

The RFID argument is especially thin. First, those chips won’t be ready to be widely deployed for several years. Secondly, their expected cost will likely make them not practical for low-priced items, and that is precisely where thieves will steal the bar codes from. But they’re not stealing the low-cost item, just its bar code.

So, the rationale of RFID-tagging only the more expensive items—and leaving the other goods to be bar code-readable—is based on the premise that someone couldn’t grab a \$300 dehumidifier and slap a \$2 stapler bar code on top of it. Clearly, the Wal-Mart case challenges that premise.

But wait, you say. If the RFID tag is on the larger item, wouldn’t that allow the scanning/reading device to identify it, regardless of whether someone has slapped a false bar code on top?

With most RFID installations, the chip must be easily deactivated so the customer can leave the store without triggering alarms. There are relatively low-cost products today that fit on a PDA and can instantly deactivate an RFID tag, said Chase-Pitkin’s Dorsey. What happens when the RFID tag is deactivated? You guessed it: It defaults to the bar code that is already on the product.

Even if retailers suddenly moved to item-level RFID tagging tomorrow, all that a theft ring would need to do is pull a PDA out of their pocket (they can pretend to be making a Treo phone call), deactivate the tag RFID, and they’re back in the bar-code world. So, that’s not really going to resolve the problem.



There are technological mechanisms that might help a little, such as using more sophisticated software that will look for product shrink patterns and then guide cameras to watch those areas more closely.

For that matter, retailers could steal a tip from the casinos and use those cameras to more closely watch the checkout lanes.

But ultimately, the technology can help only so much if you still have cashiers not paying attention. But Yankee’s Goodman suggests that they are paying attention. They are paying attention to what management tells them, and not necessarily to what the customer is doing.

The retail industry is obsessed—and rightly so—with checkout speed, and it’s nowhere more an issue than in high-volume retail locations such as Wal-Mart and major grocery chains.

“A lot of these POS systems are designed to handle 80,000 transactions a day per store. They’re designed to crank it out,” Chase-Pitkin’s Dorsey said. “There is a level of responsibility that every cashier has to assume. Clearly, these people [who scanned the bar-code fraud suspects’ items] don’t even give the time of day when it comes to work. They just push products through a scanner and collect a paycheck.”

That may be true, but part of collecting that paycheck is an agreement to listen to and comply with the priorities set by management. In this instance, retail managers might want to rethink their fraud plans and tweak their incentive triage. Otherwise, some might say that their cashier anti-theft technique is little more than a fraud itself.

# Search Engine Spam? You're Fired!

Search engine spam is a hot topic. Search engine marketing (SEM) experts far and wide hotly debate the issue. What's generally considered to be search engine spam is common knowledge to tenured SEM professionals. The major search engines publish broad guidelines regarding the SEM tactics they consider spam: Yet many highly reputable SEM firms still spam.

As a corporate SEM specialist, I've been directly involved with firing several SEM firms that have spammed the search engines.

Why would a search engine marketer put an organization's Web reputation at risk by utilizing questionable SEM tactics? The answer is obvious: It's all about profiting from others' ignorance by dancing between the lines of what's right and wrong. Why aren't the major search engines more transparent about spam penalties? Why don't they provide clear, concise definitions of search engine spam? Because the search engines can't reveal the secret ingredients that make up their algorithms. Everyone would abuse such knowledge.

When I discover an SEM firm practices questionable SEM tactics, there's only one thing to do: Fire it. Although my penalty for an SEM firm that spams the search engines is completely consistent, how I actually go about firing them varies according to the degree of their spam tactics.

## **Negligible Spam**

As an in-house SEM wonk, I'm an avowed "white hat." I employ highly conservative SEM tactics. I err on the side of caution and the desire to do right by my employer. A precise definition of search engine spam remains cloudy, but I know it when I see it.

And when I see it, I must take immediate, decisive action to undo what's been done.

If the search engine spam tactic is a relatively minor infraction, I can quickly adjust any questionable elements on a Web site and leave it to the algorithms to discover the site sins no more.

Many SEM firms will agree to work on a month-by-month basis. It's usually not worth my time or energy to confront the firm in question about its spam-like ways. If the transgression is minor, I simply allow the contract to lapse and find an SEM firm that better suits my company's needs.

## **Unembellished Spam**

If the search engine spam tactic is somewhat more severe and results in a major search engine penalizing pages within the site, I again take fast action to correct the wrongdoing, then resubmit the repaired pages to the search engines.

The more severe spam offenses are typically by sites that have undergone a complete redesign. This usually means a long-term contract with the SEM firm is in place. As SEM needs change dramatically after a site is retooled, I can usually revise the project's goals and open up bidding to other vendors.

If the SEM firm tries to stand its ground on the contract, I present it with the facts and show it the business relationship has become untenable. Usually, the firm accepts that it's in the doghouse. I'll never throw a bone its way again.

## **Egregious Spam**

If I'm called upon to resuscitate a site that's been banned by a major search engine, I hire a reputable SEM firm experienced in

reinstating wayward Web sites.

It takes a great deal of begging and groveling to get a site back into a major search engine's good graces. I must lay prostrate and bare the company's soul before the search engine that did the banning. Proper penance usually requires the assistance of a trusted expert outside the company to affirm the site has cast off its demons.

Meanwhile, I fire the SEM firm that got the site banned in the first place (of course). I complete due diligence before I confront the wayward SEM firm with a timeline of the facts. I seek legal advice, if necessary, to break any and all contracts with the firm. And I work with legal counsel to pursue damages against the rogue SEM firm.

## **Room for Improvement**

If a site is banned by a major search engine, it's because the site owner employed obvious spam tactics. Disreputable SEM firms sometimes attempt to sidestep accountability by blaming the site's owners for implementing their recommendations. A blame game ensues.

I hope some day soon definitive culpability in such matters will be determined by the courts. Unfortunately, SEM misconduct cases rarely make it out of the boardroom and into the courtroom. Corporations dread a lawsuit might reveal a lack of knowledge about a critical element of their online business. Consequently, some of the worst "black hat" search engine marketers continue to operate with impunity.

Currently, an ounce of prevention is the only defense from falling prey to marketers who spam search engines.

## Microsoft Cans Windows 2000 SP5

Microsoft has dumped the idea of releasing a fifth service pack for the enterprise-popular Windows 2000, and, instead, plans to produce an "update rollup" in the middle of next year as its last security patch for the OS.

According to a posting on Microsoft's Web site, the Update Rollup for Windows 2000 Service Pack 4 (SP4) will include all the security-related updates produced for the

operating system between SP4's release in November, 2003, and when the Redmond, Wash.-based developer finalizes the rollup's contents.

It will also contain "a small number of important non-security updates," said Microsoft.

It's taking the rollup route--which it also used in October 2003 when it released a

cumulative collection of security fixes for Windows XP--rather than a service pack, said Microsoft, because the number of not-seen-before updates are few, and Microsoft expects to have released most of them as individual updates prior to the rollup's release.

Microsoft will end support for free security fixes to Windows 2000 in June, 2005.

# Will Branded Keywords Kill Search?

I'm a little dismayed at the news regarding the recent Google trademark issue. Google can continue to initiate ads based on trademarked keywords even though it faces what amounts to a torrent of future litigation.

To summarize, auto insurance company GEICO is quite displeased with competitors bidding on GEICO-branded keywords within Google. The question is whether Google has the right to sell these terms. This is a complex problem only the Internet could create. It points to a persistent problem -- the legal world is still woefully behind the progress of technology.

## The Conundrum

We all want to let open-market forces help determine who survives with the best technology, ideas, and customer service. But, we also must respect the intellectual property of others, or we'll end up with pandemonium.

Nothing burns me more than to have a cheap competitor try to hijack a customer by leveraging my client's good name. Especially if the competitor tries a low-ball claim or provides incorrect information during the purchase-consideration process.

One thing is for sure: This problem will come to a head and have a profound effect on how search engine marketing (SEM) is sold. Major corporations will not sit around and let their highly valued trademarks be subjugated to a leveraging tactic by competitors.

## What We Must Do

First, Google must take a leadership role within the search (and really, the marketing) industry and hold a conference on the brand impact of search. Advertisers, agencies, and industry leaders need to come together to discuss the issue. If the industry agrees using

trademark terms is detrimental to brand health, Google and its peers should develop a set of policies that work for the better good.

Although common-language words will be difficult to protect, such as "American" and "United," some brand marks (GEICO, Kodak, etc.) are inherently unique and should only be made available to the trademark owner. Perhaps the industry agrees that for the right to "protect" its marks, a company should pay a reasonable fee to get that traffic. Otherwise, the terms go unsold and unlinked to the company. A win for both parties. It's up to Google to prove the value of the click to the advertiser. And it's the advertiser that will either accept or lose the valuable traffic.

Second, the major interactive trade groups -- the Online Publishers Association (OPA) and the Interactive Advertising Bureau (IAB) -- need to help steer a resolution. Otherwise, the benefits of online marketing will get mired in another silly diversion that draws attention away from the true value we've all worked so hard to nurture.

A recent study by comScore and Overture shows that only 20 percent of all online searches involve a trademark. Why not resolve these issues rather than let all search take a black eye?

A lot of our clients see great conversions from branded keywords. That tells us consumers use search as more of a navigation tool sometimes than anything else. So let's do what's right for the consumer. Let's get this issue resolved soon.

Should we just let the issue play itself out in court? Or should we take a proactive stance? How would you resolve it? Let your voice be heard.

# Accountant's Tips

With tax season right around the corner, you'll soon be inundated with forms and records from various sources. Remember that all of this information has been provided to the Internal Revenue Service. The IRS computers will be looking to match this information against your tax return. If you fail to report something on your return, it's likely that your friends at the IRS will ask why you failed to report the income or information.

Keep confirmation reports of purchases and sales of investments, including the execution prices and trade dates. Make sure the information is consistent with the information your broker will provide you on Form 1099-B. The date on which you sold securities is critical, since the new, lower tax rates for long-term capital gains apply only to long-term capital gains. But remember that this is only half of the story. You'll still have to review and research your records in order to report the purchase date and purchase price of the stock or investment.

It sounds silly, and I'm only slightly exaggerating. More and more, employers and institutions are becoming difficult in providing duplicate information (without charging a fee). And even if they are helpful and provide you a duplicate document at no charge, the waiting time involved might be extraordinary long. So it's in your best interest to review each and every piece of mail that arrives this time of the year. If you're not sure what it is, or how it might affect your taxes, simply toss it in a file for a closer review at a later date. Much better than tossing it in the "round file" and then wishing you had it when you sit down to prepare your tax return.