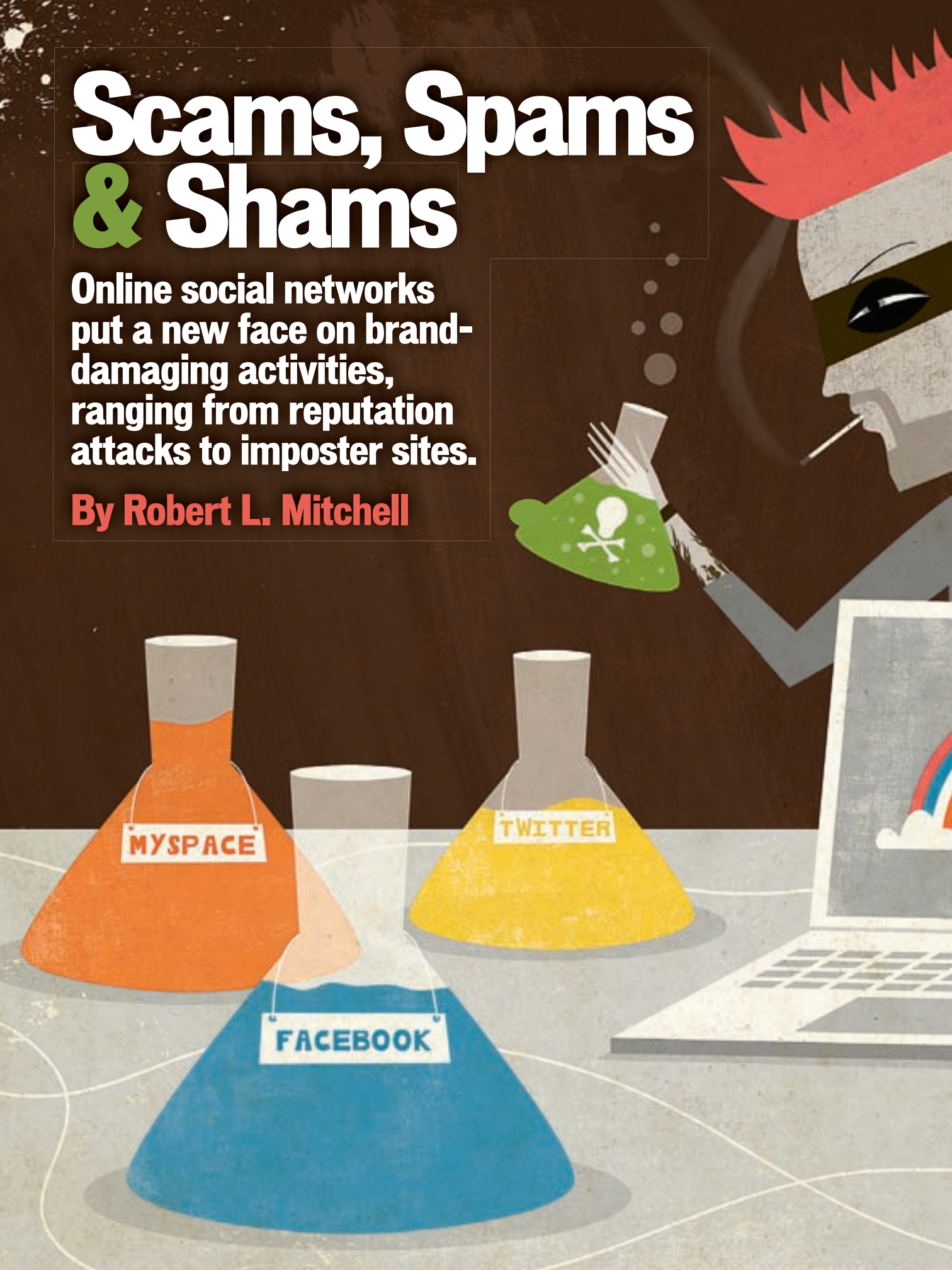
Scams, Spams & Shams

Online social networks put a new face on brand-damaging activities, ranging from reputation attacks to imposter sites.

By Robert L. Mitchell



ANDREW BANNECKER ILLUSTRATION

IT'S HARD to understand who in their right mind would want to incur the wrath of "Triple H," the intimidating superstar of professional wrestling. But when a poser created a fraudulent MySpace account in Triple H's name, it wasn't the wrestler that the perpetrator had to contend with. The smackdown came from someone who was actually watching the wrestler's back — Lauren Dienes-Middlen. She's vice president of intellectual property at World Wrestling Entertainment, the Stamford, Conn., company that owns the trademark. WWE notified MySpace, which terminated the account immediately.

The growth of social networks has brought a variety of threats that can potentially damage a brand's good name. Most of those threats aren't new, however. Social networks have simply become another attack vector, whether for spreading malware, launching assaults on an individual's or company's reputation, or creating impostor social networking sites that divert traffic away from the brand's legitimate sites.

The Triple H incident wasn't the first time that an impostor had commandeered the name of a trademarked WWE personality. "We've had a lot of impersonations," mostly on Facebook, MySpace and Twitter, says Dienes-Middlen. In fact, it's enough of a problem that Twitter recently launched an initiative to verify some accounts.

A GOOD OFFENSE

To protect themselves, businesses should defensively register company brand names and trademarks — and variations on those names — on the major social networking sites, just as they do with domain names, to protect against cybersquatters, says Pamela Keeney Lina, an intellectual property lawyer at Alston & Bird LLP in Atlanta, who has written about protecting intellectual property on social networks.

Social media cybersquatting is where domain name cybersquatting was 10 years ago, says James Carnall, manager of the cyberintelligence division at security monitoring firm Cyveillance Inc. People use variations on brand names to open accounts on social networking sites, in hopes that companies will pay them to relinquish control of the accounts. He points to the online market Tweexchange as a prime example of how trading in social network names is a growing business. Unlike domain names, however, social networks have no central authority like ICANN or established processes for reclaiming brand names from cybersquatters.

"Our most valuable asset is our intellectual property. You have to protect [it] or you lose your rights to it.

LAUREN DIENES-MIDDLEN,
VICE PRESIDENT OF INTELLECTUAL PROPERTY, WORLD WRESTLING ENTERTAINMENT

Some impostors are simply overzealous fans, but Dienes-Middlen is more concerned about scammers and those who sell pirated videos and poor-quality knockoff WWE merchandise, which robs the company of revenue and cheapens its brands. Those sites lure users through social networks, spam, abusive search engine marketing and other channels. Last year, WWE shut down 3,200 online auctions of phony WWE products with an estimated street value of $16 million to $33 million. During one Wrestlemania pay-per-view event this spring, WWE was able to use social networking sites to identify a number of unauthorized Web sites that planned to stream the event

live. It also found 8,600 sites that had made pirated copies or footage of the event available after the fact. "Counterfeiting operations are highly organized, are very global and are picking up steam because of the economy," says Liz Miller, vice president of the Chief Marketing Officer (CMO) Council.

THE COST OF PIRACY

Online counterfeiting also damages brands in other ways. For example, some people who buy pirated copies of Microsoft Corp.'s Windows operating system may think they have legitimate copies, says Cori Hartje, senior director of the Microsoft Genuine Software Initiative. What they get is software that often includes embedded spyware and malware — and they expect Microsoft and its channel partners to support the product. Hartje says she's seen research showing that counterfeiters today can make more money from the spyware and malware than they get from selling the pirated software itself. Meanwhile, the user blames Microsoft for any problems the malware causes. "That hurts our brand," Hartje says.

At WWE, while the onus is on the corporation itself to find and shut down sites peddling pirated videos and other counterfeit wares, most sites do try to cooperate. Many video-sharing sites, such as YouTube, have tools available to report and take down footage that violates copyrights.

Dienes-Middlen says the challenge isn't shutting down the sites that WWE finds, but keeping up with the new ones that continue to crop up. While businesses can assign employees to do that, she recommends trying a third-party monitoring service to get a handle on the problem. Dienes-Middlen thought she had things under control — until she did a test run with brand protection service MarkMonitor Inc. The losses WWE had uncovered on its own were just the "tip of the iceberg," she says.

Soon afterward, she went to WWE's chief operating officer to ask for additional funds to clamp down on the illicit activity. "This was something we needed to attack. Our most valuable asset is our intellectual property," Dienes-Middlen says. "You have to protect [it] or you lose your rights to it."

VISITORS UNDER ATTACK

HERE'S THE SCENARIO: Attackers compromise a major brand's Web site. But instead of stealing customer records, the attacker installs malware that infects the computers of thousands of visitors to the site. The issue goes unnoticed until it's exposed publicly.

Such attacks are a common occurrence, but most fly under the radar because the users never know that a trusted Web site infected them, says Brian Dye, senior director of product management at Symantec Corp. When his company tracks down the source of such infections, it often quietly notifies the Web site owner. But word can get out, leaving the Web site's customers feeling betrayed, and seriously damaging a brand's reputation.

Attackers, often organized crime rings, gain entry using techniques such as cross-site scripting, SQL injection and remote file-inclusion attacks, then install malicious code on the Web server that lets them get access to the end users doing business with the site. "They're co-opting machines that can be part of botnets that send phishing e-mail, that are landing sites for traffic diversion and that host malware," says Frederick Felman, chief marketing officer at MarkMonitor. But because the business's Web site isn't directly affected, the administrators of most infected Web sites don't even know it's happening.

That possibility is one of Lynn Goodendorf's biggest worries as global head of data privacy at InterContinental Hotels Group. "I worry about attacks that use a combination of malware and botnets," she says, adding that she has watched this type of activity increase steadily over the past two years. "That's very scary," says Goodendorf.

Most victims haven't associated such attacks with the Web sites that inadvertently infected them. But that may be changing.

The latest versions of Microsoft's Internet Explorer browser and Google's search engine detect sites infected with malware, issue a warning and block access to the site. "To me, this is serious online brand damage," says Garter analyst John Pescatore, and it can be disastrous for small and midsize businesses that totally depend on search engine traffic. The next frontier, says Dye, may be attackers who use these types of exploits against the Web sites of high-profile brands and then publicize – or threaten to publicize – what happened.

Preventing attacks like SQL injections requires using enterprise-class security tools, such as intrusion-prevention and -detection systems, with a focus on behavioral analysis to spot attacks, Dye says. But Pescatore sees a more fundamental problem: rushing through Web site updates and ignoring development best practices designed promote security. Most organizations follow formal processes for major upgrades, but not for the constant "tinkering" that takes place. The result: Vulnerabilities creep into the code. "Security groups often are forced to put Web application firewalls in front of Web servers to shield [these] vulnerabilities from attack," says Pescatore.

– ROBERT L. MITCHELL

Social networking sites can be a launch pad for reputation attacks from competitors, customers or disgruntled employees. Jeff Hayzlett, chief marketing officer at Eastman Kodak Co., says he has seen competitors try to hijack conversations — sometimes anonymously — with customers on the company's Twitter and blog sites.

In one Twitter exchange between Kodak and a prospective customer, a competitor jumped in and "inundated" the inquirer with negative comments about Kodak's product while promoting his own company's offering. It was, Hayzlett says, "a rude way to participate." He has a name for Twitter users who employ such tactics: He calls them "twankers."

Any time you sell a product or service, you're going to have issues like this, Hayzlett says, so Kodak hired a "chief listener." That person monitors all conversations and routes problems to the appropriate group, be it legal, IT or marketing, so that the company can follow up. When a customer is publishing negative comments, he says, his preference is to have a private conversation rather than use a public forum.

Other threats can be self-inflicted. Hayzlett himself admits to prematurely posting a tweet about the impending retirement of a product. "I accidentally

hit Send instead of Save and tweeted out what we had worked six months to protect," he says. In the time it took to delete the tweet, four people had retweeted it. "I had to reach out to them and beg them to [remove it]." Even then, the tweet may have shown up in Twitter searches.

Gartner Inc. analyst John Pescatore says a client that runs a campground chain had an employee who thought he'd be helpful by posting a spreadsheet on Facebook that showed which sites were available and which were booked — but it included the credit card numbers campers had given to reserve their sites. Data-leak prevention tools won't find such data when it's posted outside a corporate firewall. With social networks, "periodically looking at content has to be part of the cost equation," Pescatore says.

Some threats come from inside. In an April survey of more than 2,000 U.S. employees and executives by Deloitte LLP, nearly three quarters of the employees said that it was easy to damage a company's reputation using social media — and 15% said they would post comments online if their company did something they didn't agree with. That could be a big problem for WWE, since employees who know the storylines of its scripted events could spill the beans. "If those outcomes were revealed, it would destroy the experience for the fans," Dienes-Middlen says, so all WWE employees are required to sign confidentiality agreements.

DIVERSIONARY TACTICS

Social networks also have been used by scammers to lure a brand's customers to malware or phishing sites — or to e-commerce sites hawking counterfeit or gray-market products. According to a survey by MarkMonitor, which tracks online threats for its clients, in the 12-month period ending in the second quarter of this year, phishing attacks on social networking sites increased by 164%.

In a CMO Council survey of 4,500 senior marketing executives, nearly 20% of the respondents said they had been affected by online scams and phishing schemes that had hijacked brand names. It was the third-biggest category, right behind cybersquatting or illegal use of a trademarked name, and the illegal copying of digital media content. The fourth category was online sales of fake products that contain deficient or dangerous ingredients.

Barbara Rentschler, CMO at K'nex Brands LP, sees cybersquatting, online scams and false association of its brands on other sites as the biggest threats to the toy maker's brands on the Web. She uses a monitoring service to track and shut down cybersquatters and scam sites. Many sites that misappropriate K'nex trademarks are overseas, she says. Most aren't malicious: They're simply businesses that hope to become K'nex distributors.

With so many different brand threats to contend with online, it's important to have a coordinated strategy. Unfortunately, says Cyveillance's Carnall, many organizations take a triage approach, sending the issue to legal, IT or marketing. "They silo it," he says. But someone needs to be keeping track of outcomes and the overall impact on the brand, he contends. "You almost need a brand intelligence officer."

At Kodak, the buck stops at the CMO's desk. Hayzlett keeps communication flowing through what he calls online councils with every department in the organization, including IT, legal and human resources. "Everyone needs to work together and understand each role. We work as a team," he says.

Communication between marketing and IT is key. "The most powerful team would be if you connected the CMO and the CIO at the hip," Miller says.

Customers are often the first to notify a business of a problem, so listen to customer service lines carefully, says Frederick Felman, CMO at MarkMonitor. At WWE, it was fans, not staffers or a monitoring service, who first reported the Triple H imposter. "Take the complaints you get seriously," Felman advises, "and be prepared to act quickly."

Rentschler says IT needs to educate colleagues in marketing about risks. If IT sees a problem and fixes it without telling anyone, "no one else will know what to look out for," she warns.

IT needs to push back more when marketing plans can jeopardize brand security. It must, for example, fight pressure to rush Web site changes through without thorough security checks. "I don't think IT does a good job of saying, 'Here's all of the IT issues with the brand upkeep,' " Rentschler says.

With so much online turf to monitor and so much activity in cyberspace, it's important to prioritize. Lynn Goodendorf, global head of data privacy at U.K.-based InterContinental Hotels Group, says she tries to focus on sensitive, confidential data. But even there, you have to have realistic goals. "Mitigate your largest exposures," she says, "but don't think you can mitigate it down to zero." ■

REACHING OUT

The most popular uses of social networking among businesses:

Building awareness of our corporate brand	62%
Communicating with clients	62%
Searching out new business leads	40%
Helping employees collaborate/communicate	40%
Recruiting new talent/ finding workers	33%
Building a customer service community	29%
Conducting market research	23%
Conducting background checks on job candidates	17%
Creating an alumni network of former employees	15%

Base: 52 IT professionals participating in an exclusive *Computerworld* survey who said their organizations use social networking, September 2009

CHATTERBOXES

A bevy of social networking tools are being used at the corporate level:

Instant messaging	49%
Organization-sponsored social networking groups	34%
Blogs, wikis or forums	32%
Employee-created social networking groups	30%
Video-sharing sites	20%
Content referral sites	10%
Photo-sharing sites	8%

Source: Exclusive *Computerworld* survey of 120 IT professionals, September 2009