

Protecting Your Good Name in Cyberspace

Who steals my purse steals trash," said Iago to Othello. "But he that filches from me my good name . . . makes me poor indeed."

Four hundred years later, a good name is still priceless, but on the Internet, trashing that good name can cost as little as \$8.95. From Juniata College in Pennsylvania to Reed College in Oregon, from the NCAA to the White House, Webmasters have puzzled over reports that their home pages have mysteriously turned into distribution centers for pornography, gambling, or outrageous social commentary. No, their Web sites have not fallen prey to the latest virus. Instead, unsuspecting surfers inadvertently have landed—by typographical error or bad guesswork—on a URL slightly different from the one they wanted.

In the case of college and university Web sites, the simplest alteration is the substitution of ".com" for the correct ".edu" suffix. Earlier this year, Juniata College administrators discovered that www.juniata.com directed browsers to a pornography site. A year ago the University of North Carolina confronted sexually explicit material on www.uncgirls.com. An Internet gambling site is located at www.notharvard.com. Louisiana State University is suing one of its own students over www.lsulaw.com. Even the most powerful institutions are not immune: neither www.whitehouse.com nor www.whitehouse.org features content that the management of www.whitehouse.gov would find acceptable.

What's behind these rogue pages? Some cases are perfectly legitimate: the Web site owners have no intent to deceive

the public or to trade on the name of a better-known institution. When Harvard University objected to the Internet name of Harvard Pilgrim Health Care, the Massachusetts attorney general weighed in on the side of the decades-old HMO, and www.harvardpilgrim.org remains on the Web today. But in other cases, the goal is a satire of or a grievance against the holder of the legitimate site name. The Web site www.bsupolice.com presents its owner's case against the campus police department of Ball State University. Though such Web sites are hard to shut down, a targeted college or university should be able to insist on a prominent statement that the site is not affiliated with the institution.

Sometimes the motivating factor is to generate traffic from the inevitable finger-slips (www.micorsoft.com) or to imply a connection with a well-known organization. An anti-abortion group registered a site name suggesting an affiliation with the Brookings Institution, and the NCAA is in constant pursuit of such names as www.ncaareresults.com and www.ncaafootballodds.com. Legal techniques can be effective here, based on conventional fraud and trademark law and also on the Uniform Dispute Resolution Policy (UDRP), which all domain-name registrants must agree to follow.

Finally, some companies register names solely for the purpose of selling them to the organizations that already identify with those names. Several years ago, this type of activity was common. Cybersquatters routinely contacted colleges and universities with offers to sell the ".com" versions of their names. With the passage of the Anticybersquatting Con-

sumer Protection Act at the end of 1999, however, it became illegal to register a domain name solely for the purpose of selling the name to someone with a prior trademark claim.

Suppose a college CIO discovers one of these Web sites. What should the CIO do? Just as misuse of the college logo on a T-shirt would not be considered an issue for the textile arts department, misuse of the college name on a Web page is not primarily a technology issue. The college attorney, the public relations director, and the trademark and licensing manager "own" this problem. They will ask questions like these: Is the site trying to make money by trading on the college name? Is it deceptive or fraudulent? Does it make use of college trademarks, logos, or identifiable images? Does it fall under the "bad faith" provisions of the 1999 anticybersquatting legislation? The role of the CIO will be to explain the basics of the domain name system, including how names are registered. The CIO should be prepared to differentiate between the owner of the name, the owner of the computer pointed to by the name, and the owner of the Web site to which the initial URL is redirected. Any or all of these owners, along with the ISPs that connect them, are likely targets of cease-and-desist letters, lawsuits, or arbitration requests.

For higher education institutions, the struggle can be long and expensive and may end in compromise rather than complete victory. But Shakespeare would advise staying the course: your good name is worth the trouble.

Steve Worona is Director of Policy and Networking Programs for EDUCAUSE.