Lesson 1

Cybercrooks profit by 'squatting' on brand names

By Theresa Howard
USA TODAY

As advertisers spend more online, brand name firms increasingly are seeing their names, customers and millions of dollars in sales hijacked by shady marketers.

Instances of deceptive marketing to build traffic for rogue sites or to sell faux-branded products rose 17% last year, according to MarkMonitor, whose software tracks digital marketing infringement.

Shady marketers are using so-called cybersquatting to do their digital stealing. They drive people to a "squatted" site via e-mails or through paid search. Once they've led someone there, they hope to steal credit card information, spur clicks on ads to skim revenue from online ad networks or sell fake products, such as pharmaceuticals or pricey handbags.

The tactics target electronics, sports apparel, luxury brands and pharmaceutical brands the most and cost marketers about $175 billion worldwide in lost revenue, says Fred Felman of MarkMonitor.

"When the economy goes south, white-collar criminals don't quit," Felman says. The company's "Brand Jacking Index" report shows that daily incidences of cybersquatting against 30 of the top global brands rose to 449,484 last year vs. 382,246 in 2007. A first-time study coming out today in conjunction with industry group Chief Marketing Officer Council addresses how marketers are coping with the surge in cybersquatting.

"We're at a point in which marketers need a wake-up call in what's happening to their brand," says Liz Miller, vice president, programs and operations for the council. "Marketing is in the dark, and cybercriminals are ramping up their game."

Incidents are up as marketers increasingly use search engine optimization to reach consumers online, where ad spending is expected to top $24 billion this year. While ad expenditures overall are expected to fall by as much as 10%, digital advertising in 2009 is expected to be up about 4.5% over 2008, according to online marketing tracker eMarketer.

As businesses fight for a share of dwindling dollars, rogue marketers are getting more aggressive. The CMO study says that marketers see their brands as more vulnerable to infringement online than in other media, with 29.5% of the 300 marketers reporting brand infringement on the Web vs. 22.6% in other media.

Despite the big cost to marketers, few of them invest in protecting their brands online. The CMO study reports 52% of respondents spend less than $100,000 on brand protection annually. Just 2.7% say they spend $5 million or more.

As seen in USA TODAY May 11, 2009

Lesson 1

Introduction

The reprinted article on the first page of this lesson focuses on cybercrooks who use online marketing to lure unsuspecting customers away from brands' real websites to fake websites. Taking advantage of a name brand by building a website that seems like the brand's real site is called *cybersquatting*. Once a person is lured to the site, the cybercrooks do one of several things: steal the customers' credit card information, sell fake products or promote clicking on ads to take revenue away from pay-per-click online marketing networks. Read the article on the first page of this lesson and then answer the discussion questions below.

Discussion

1. How concerned should brand name firms be about cybersquatters?
2. How do cybersquatters operate?
3. What signs might indicate that a website is the handiwork of a cybersquatter?
4. Why do you think companies are increasing spending on digital advertising, while expenditures for ads overall are dropping? How does this increase affect cybersquatters?
5. What are the characteristics of a "rogue marketer"?
6. How are consumers affected by cybersquatters?
7. If you were a marketer, how would you combat the increase in cybersquatting?

Activity

In the article, Liz Miller of the Chief Marketing Officer Council says, "Marketing is in the dark, and cybercriminals are ramping up their game." Conduct 10 minutes of online research and come up with a solid definition of the term "marketing." Then, in small groups, visit the website of Ogilvy & Mather, one of the world's most renowned advertising, marketing and public relations firms (www.ogilvy.com). Click on "capabilities" and read about the different kinds of marketing the firm provides. Next, choose five of the types of marketing listed. For each, explain how a cybercriminal could exploit it. In the grid below, create a cyber term for each kind of underhanded marketing and describe it. (For example, *squatting* is living on someone else's property without permission or payment; *cybersquatting* is using someone else's domain name to make money.)

Type of marketing	Name/description of exploitation

Finally, adopt the role of cybersecurity advisors to a brand name firm who is "in the dark" and develop at least one way that the company could deter cybersquatters.

TEACHER'S GUIDE

Lesson 1

Overview:

In this lesson, student groups will:

- Read about how cybercriminals are exploiting the domain names and products of big brands.
- Identify the possible signs of cybersquatting.
- Define marketing and identify different types of marketing.
- Determine how cybercriminals could use five different types of marketing to their advantage.
- Role-play cybersecurity experts and develop ways to deter cyberattacks on a brand name firm.
- Ascertain ways to safeguard against cyberattacks on U.S. supply chains.

Grade level:

6-12

Subject areas:

career and technical education, language arts, social studies, advisory classes

Time requirements:

Step 1: Read the introduction to the lesson (Page 2), and then read the article (Page 1) (10 minutes).
Step 2: Answer the discussion questions (15 minutes).
Step 3: Conduct Internet research on the different types of marketing (20 minutes).
Step 4: Work together to complete the grid (30 minutes).
Total: 75 minutes (Note: Times may vary according to students' ability levels.)

Notes:

1. Ensure students have a good understanding of cybersquatting before you read the article. Consider reading the article as a class, as there are many terms students may be unfamiliar with. Briefly review the following terms used in the article: brand, marketing, rogue site, faux-branded, squatting and media. Also ask students if they have had any experiences with squatted sites.

2. Students can find a thorough definition of marketing as individuals or in their groups. They should visit the Ogilvy & Mather site in their groups, so that they can choose which types of marketing to focus on.

3. Encourage students to be creative when making up names for the exploits they have developed. The names can each begin with "cyber" but don't have to.

Links:

- National Cyber Security Alliance — StaySafeOnline www.staysafeonline.org
- The Department of Homeland Security's Critical Infrastructure/Key Resources Protection Resources www.dhs.gov/xprevprot/programs/editorial_0211.shtm
- Transportation Security Administration www.tsa.gov
- Federal Trade Commission: OnGuardOnline onguardonline.gov
- United States Computer Emergency Readiness Team www.us-cert.gov
- i-SAFE www.isafe.org
- Wired Safety Organization www.wiredsafety.org

- Federal Trade Commission: OnGuardOnline onguardonline.gov
- Multi-State Information Sharing and Analysis Center www.msisac.org/awareness
- i ConnectSafely: www.connectsafely.org/safety-tips-and-advice.html
- i iKeepSafe: http://tools.ikeepsafe.org/older-students

Industry association links:

- A public service website sponsored by Internet industry corporations and public interest organizations www.getnetwise.org
- The Anti-Phishing Working Group (APWG) www.antiphishing.org
- Direct Marketing Association www.the-dma.org/index.php
- The Sans Institute www.sans.org
- The Computing Technology Industry Association www.comptia.org

