Managing Online Promotion Security Risks

Vandana Taxali, J.D., LL.B., Legal News Contributor
PubZone

March 4, 2005

Security issues are a growing concern for online promotions - and comprised a hot topic at the Canadian Institute's 11th Annual Advertising and Marketing Law Conference, January 25-26/05.

Online promotions allow companies to be more innovative, edgy and savvy with their promotions. However, as modern technologies continue to evolve, so do new challenges associated with interactive promotions that did not exist with traditional paper-based promotions, Duncan McCready, executive vice-president, IC Group Inc., told delegates. Consequently, the growth of promotions conducted online also results in the increase in security threats.

All parties, including advertising agencies, promotional agencies, contest administrators, contest sponsors, law firms, promotional insurance providers, interactive agencies, hosting facilities, and any other entity involved in the promotional contest implementation process need to be concerned with the management of security risks and involved in preventative measures.

McCready pointed out the following external security threats with online promotions:

- Phishing – the creation of e-mail messages and Web pages that are replicas of existing Web sites so as to mislead consumers into submitting personal information;
- Spam – the bulk distribution of unsolicited e-mails, thereby making it unappealing for consumers to receive marketing information via email;
- Denial of Service Attacks (DOS) – mass traffic on a Web page that can cause hardware to crash and cause Web sites to take a longer time to load or come to a complete standstill altogether;
- Robots – machine readable code which can simulate a real user, and can be used to enter promotions thousands of times faster than real people within short time frame. –This can create a disadvantage for entrants who enter via non-mechanical means, and it can slow sites the way DOS attacks do;
- Subversive Data Insertion techniques – data posting source code of promotions can be subverted and code can be created so that date is entered directly into the promotion without properly entering via the contest Web site;
- Unsecured Flash or other client side code: hackers may decompile flash movie files or unsecured source code for clues as to how sites function or manage data with databases;

Hackers are a real legitimate threat to online promotions as they can also unleash viruses, interfere with your contest entrant database, obtain personal information from entrants and damage entrants' computers when information is downloaded.

There are also internal security threats from IT or other staff who may circumvent security protocols by allowing unauthorized access to the promotion or sharing confidential contest data. There could also be software programming problems that don't save all entrants' data information.

To avoid and manage online promotional risks, McCready recommended a number of extremely helpful preventative steps. He emphasized the importance of developing an initial list of controls and procedures with all promotion partners which include: communicating areas of risks to all required parties; appointing a point person who is responsible for ensuring that process, implementing security and control functions; having the most secure technology available; protecting consumers privacy rights; and ensuring that security and control functions aren't executed by one individual.

McCready's company, IC Group Inc., also provides prize insurance. Therefore, if a glitch in the computer software tells all entrants that they are winner and a contest sponsor is held liable to provide a prize to all entrants, a contest sponsor would be able to deal with the unexpected out-of-pocket expense of awarding all the prizes - thereby avoiding any negative

publicity.

Beyond the internal controls and procedures that McCready recommends, a pre-planned public relations strategy and proper contractual legal safeguards can also help minimize security threats.

Legal liability and negative PR are the biggest concerns for any online security risks to a promotion. A PR nightmare can leave a bad impression in the minds of consumers for a long time that may be difficult to erase. Therefore, a company should always have a PR plan in place prior to beginning an online promotion. Such a plan would include how to deal with contest entrants, winners, and the public at large.

A company should be able to communicate with the public at a moment's notice, whether via Internet (including dark sites), phone or traditional media (print, radio and television).
Dark sites are particularly useful - these are web pages that have been designed in advance in preparation for a crisis that are not accessible to the public and kept "dark" or hidden until needed during a security crisis. Then, if a crisis situation transpires, a company will already have web pages dealing with the security issues prepared in advance.

The Media Relations conference organized by The Canadian Institute on March 01-02/2005 at the Four Seasons dealt with this issue in the session, "Crisis Communications: Managing Issues and Overcoming Crises", speaker, Brian Lambie, Principal, Redbrick Communications says that the elements of a good public relations plan include: identifying risks; clarifying policies; roles and responsibilities; establishing a permanent crisis response team; providing effective staffing; training and resources; and training an appropriate spokesperson. Building relationships with reporters and creating a list of academic experts are also good ideas for preparing for a potential security risk.

Carefully worded legal clauses in the contest rules can also help minimize any liability in the event that there are security breaches. Among these would be clauses that:

- avoid any legal liability in the event that there are any glitches in technology;
- allow the temporary suspension of the contest for any reason;
- deal with breaches of privacy;
- deal with computer glitches;
- deal with interference by third party hackers;
- minimize legal liability for any errors or omissions by co-sponsors;
- would ensure that co-sponsors adhere to all applicable laws
- prohibit entrants from entering a contest through automated means

And more.

All these elements – internal controls and procedures, pre-planned public relations strategy and legal protections will all help make sure that your promotion runs smoothly and avoiding the high costs associated with a promotion gone awry.