

New Twist on Phishing: How e-Mail Marketers Can Deter Brand Attacks

By Rick Buck, Director of Privacy and ISP relations, e-Dialog

Overview

New phishing techniques for deceiving consumers are on the rise and have been making headlines in the industry trades and national media. The Anti-Phishing Working Group reported that the number of phishing spoof sites reached an all-time high in January 2007, and among the brands and legitimate entities hijacked by e-mail phishing attacks there were numerous non-traditional Web sites spoofed. Whereas phishing has been targeted primarily at the financial services sector, if left unguarded these brand attacks have the potential to create major problems for many other important sectors, including retailers, healthcare/pharmaceutical and travel companies.

New phishing techniques

The latest phishing technique is called image-based spam. Much like it sounds, the e-mail is a single image that looks exactly like your brand or no brand in particular. It is laden with randomly dispersed clear pixels so that it looks different every time spam filters see it and therefore difficult to detect. This has become very popular in industries like pharmaceuticals (to sell fake drugs) and financial services (to illegally inflate stock prices a.k.a. - pump & dump scams).

Another new and more concerning technique is to mimic newsletters or other e-mail messages from legitimate companies. The fake e-mail messages look exactly the same as the real ones because they contain actual stolen content and links from the original e-mail. The only differences are hidden malicious phishing code, or links to phishing sites that attempt to plant viruses on the recipients' computers.

How to deter them

While it is virtually impossible to prevent phishing attacks, e-mail marketers can deter them and/or reduce their effectiveness by taking a few simple precautions.

1. Authenticate. Authentication with all the leading technologies, including Sender Policy Framework (SPF), Sender ID Framework (SIDF), Domain Keys and DKIM, is a strong deterrent to catching fake e-mail at the ISP level. If authentication checks fail, the ISPs are likely to filter e-mail away from inboxes or block it completely. This will reduce the effectiveness of phishing attacks and enhance deliverability with many ISPs. Notes:

- *Marketers need to use marketing and corporate sub-domains specific to their brands so that all authentication schema can be utilized by both corporate and marketing IP addresses and domains.*
- *Domain Keys authentication will also be a qualifier for the Yahoo feedback loop program.*



2. Certify. Certification services like Goodmail, SenderScore or Habeas put e-mail under further scrutiny at the ISP level, ensuring that only legitimate mail is delivered by the respective ISPs. While there are varying opinions about the need for these services they add credibility and integrity for ISPs as well as authenticity for recipients.

3. Educate consumers. It is important that customers are able to distinguish fraudulent e-mail from real e-mail and Web pages they are directed to. Specific recommendations include:

- *Ensure privacy policies specifically state who sends e-mail on behalf of the brand.*
- *Tell customers what IP addresses and domains they should expect to see and where to look for them.*
- *Let customers know exactly what information will always or never be included in e-mail messages.*
- *Build a consumer protection Web page to speak about phishing attacks and other fraudulent behavior. eBay has done a particularly good job presenting this information to their users.*

For more information on this or other deliverability-related subjects contact Rick Buck, director of privacy and ISP relations for e-Dialog: 781-372-3317 or rbuck@e-dialog.com