

DIRECT®

The Magazine of Direct Marketing Management

Good Web-keeping Seal Helps Small Brands

BY BRIAN QUINTON

BETWEEN PHISHING, PHARMING AND flat-out flim-flammy, the Web is beginning to look like a much less trustworthy place for consumers to transact their business. A February 2005 survey by security provider RSA Technologies suggested that one-quarter of Internet users may have cut back on their online shopping out of fears for the security of their personal information—their credit card numbers, social security data, bank accounts or even just their e-mail address. That's not a problem if you're an established and trusted brand name, working off the large fund of credibility and goodwill of, say, an Amazon.com. But what do you do if you're a small online merchant, a niche retailer or a start-up? How can you convince potential first-time users that you're committed to handling their data safely and conscientiously?

One route to credibility is to join a privacy seal organization and display a symbol on your Web site that denotes good stewardship of your customers' data. Larry Ponemon, president of The Ponemon Institute and a consumer privacy expert, puts it bluntly: "If you're collecting customer information on the Web and you're not showing some membership in a privacy watchdog organization, then shame on you." In the current climate of heightened awareness about identity theft, that omission could lose you sales to a competitor with a clear—and visible—data protection policy.

TRUSTe is an independent non-profit organization that operates privacy certification and seal programs for 1,300 sites around the Web. Many of these are large companies in the technology space: AOL, Microsoft, Intuit, and IBM. Others are big corporations facing the consumer more directly: The New York Times, The Carlson Companies, Intercontinental Hotels, Holiday Inn.

But the majority of those 1,300 sites belong to small to mid-sized companies, says Fran Maier, president and executive director of TRUSTe. These companies may be far from having the largest market share in their field; in fact, they may not have a profile that could be called a "brand". And for that reason, they see wisdom in compensating for that by offering customers the extra assurance that comes with a deal of good privacy conduct from an organization like TRUSTe.

"We've done some research on this and found that for many small companies, their brand does not say a lot about trust or privacy," says Fran Maier, president and executive director of TRUSTe. "Smaller companies often see joining us as a way to build brand value, trusted relationships with consumers, and in the end higher transactions." While the big companies can pay as much as \$75,000 in annual fees for the right to display the TRUSTe seal, Maier says the organization has a stepped membership fee that can be as little as \$600 a year for small operators.

Of course, the seal is only the outward symbol of a lot of hard work invested in safeguarding the privacy and security of consumer data. In order to be certified by TRUSTe, Web companies have to design, publish and abide by a privacy statement that makes clear what they do with the information that they collect online. They must agree to give their customers a choice as to whether that information will be sharing with third parties for marketing purposes, and to agree to dispute mediation in cases where customers feel their information has been used unfairly. Many small Web operators don't have the in-house legal chops to draw up these policies on their own. In those cases, TRUSTe can offer guidance and counsel in constructing a clear, effective privacy policy.

Once a Web merchant has signed on and been certified, TRUSTe stands between that merchant and the customer, checking regularly to make sure the site's privacy practices match the privacy statement. Maier says that about 10% of applicants for TRUSTe certification don't actually wind up completing their applications, and the organization terminates about one membership a year for non-compliance.

"Some of our recent terminations were among smaller companies, and I think they occurred because these companies didn't realize that we would be monitoring their compliance. I think that some companies actually do want to spam their customers and just want

to seem trustworthy. Unfortunately, that's not a practice we can get behind."

Apart from the Web seal, TRUSTe members are kept apprised of legal and technological developments in privacy protection, on both the state and federal levels—something that can be hard for a small Web business to monitor but crucial to know, given the Internet's mass reach.

Consumers can click on the TRUSTe seal when they find it on a Web site and find out more information on the site's privacy and data protection policies. They can also filter on the seal when looking up merchants in some shopping comparison engines such as Shopzilla.

TRUSTe administers several other certification programs dealing with online privacy and user protection. In fact, the organization is working on developing another seal program aimed at small online companies that want to solicit e-mail permissions. Called a "point of collection" seal, this symbol would be displayed at whatever point in the Web site offered the user an opportunity to sign up to receive communications. "It would say, 'When you sign up here, you're not going to get spammed,'" Maier says. "One of the biggest issues for Web companies is getting permission to send e-mail. This basically lets consumers sign up for e-mail from the site and still be confident that they're not going to get anything else." TRUSTe also performs the certification called for under the Bonded Sender e-mail program, in which companies vow not to spam and post a monetary bond as pledge of their intentions.

In addition, Maier says, TRUSTe considers it important to take part in the many discussions now going on about privacy policies, both among Web merchants and in the offline world, where companies amass data about consumers as a by-product of doing business. Last week, the organization issued a set of guidelines for consumer data handling and is now soliciting comment from its members. Those high-level best practices include training all employees in a company-wide security policy data; "need to know" access procedures within the company; encryption of data sent across public networks, especially via wireless LANs or Bluetooth; and regular tests and monitoring to make sure procedures are being followed.

Admittedly, it's hard to set data protection guidelines that will cover all TRUSTe members, simply because their needs and risks are so various. A large financial site will have to dedicate many resources to implementing safe data collection and storage; a small Web merchant may only need to make sure not to ask for more information than he or she needs.

Other guidelines put out by the group speak more directly to small and mid-sized Web operations. In early April, TRUSTe responded to new virulence in the phishing epidemic by collaborating with Ernst & Young on a white paper about reassuring customers against identity theft. Entitled "How Not to Look like a Phish", the paper gives tips on how to avoid tactics that phishers commonly use in their scams, either through e-mail or on the Web.

These include:

- Don't request customers' personal information directly from an e-mail hyperlink.
- Don't use "Click Here" hyperlinks; direct customers to your Web site with a visible URL.
- Personalize the body of the e-mail message with non-threatening detail, such as a first or last name. (But not in the subject line—a spammer's trick.)
- Be careful about applying time challenges or restrictions to your messages. Phishers usually flag their messages as "urgent" and ask for immediate responses, to get the biggest haul they can before they're detected.
- On the Web, make your domain names are clean-cut and crisp; don't send customers to Web sites via complex domains or IP addresses—a tactic phishers use to get around the hurdle of domain name servers.
- Don't use pop-up windows for data collection, especially those without address bars or navigation elements. Some fraud artists gather ID data by applying fake pop-ups to legitimate Web sites.

Web merchants who adhere to these suggestions will not only avoid the taint of fraud in their own customer contacts but will help consumers break the bad online habits that often make them prey for scam artists and ID thieves. "That helps everyone in the end—merchants and consumers, large and small," Maier says. **D**

Reprinted with permission from the April 27, 2005 issue of *Direct*® (www.directmag.com)
Copyright 2005, PRIMEDIA Business Magazines & Media Inc. All rights reserved.



685 Market Street, Suite 270
San Francisco, CA 94105
(415) 520-3405

DRT-57-EK