Are You Exposing Your Online Donors to Credit-Card Thieves?

Before you accept donations online, be sure people's credit-card numbers are secure.

By David Crooke

Online marketing techniques have revolutionized the world of nonprofit organizations. As more people integrate the Internet into their lives, nonprofits need to understand the advantages of using Web technology to streamline donation processing.

Online donation processing is an excellent way to reduce costs and manual tasks associated with direct fundraising. However, using the Internet for donation processing requires stringent security processes. Here are a few key issues to consider:

SSL Doesn't Necessarily Make It Secure.

Many people talk about their "secure" Web sites when they actually mean that the communication between the Web browser (such as Microsoft Internet Explorer® and Netscape®) and the Web server is encrypted using the Secure Sockets Layer (SSL), a standard set of Internet communication rules for managing the security of message transmissions over the Internet. While using SSL is essential, it's just one minor element of an overall security architecture.

> About 80% of successful online "break-ins" involve simply stealing passwords to gain access.

> While using SSL is essential, it's just one minor element of an overall security architecture.

People who hack, or break into, Web servers typically don't do it by tapping into connections from browsers. Instead, they do it by attacking other weak points, including the human element. In fact, about 80%* of successful online "break-ins" involve simply stealing passwords to gain access. Therefore, any organization should carefully consider end-to-end security processes before offering online donation processing on its Web site.

* Data from Carnegie-Mellon CERT Advisory Center.

Should You Store Credit Card Numbers?

Another key concern is securing credit card numbers once the Web site has accepted them. Smaller e-commerce software providers are often lax about this aspect of security, so organizations should be careful to understand a provider's security policies before using its services for online transactions.

In addition, many organizations encrypt their Web databases, mistakenly believing that this protects the data. However, hackers who break into a server get not only the encrypted data but also the decryption keys and software, enabling them to obtain the card numbers. There is also the risk of a security breach if credit card information is available to staff members.

> Many organizations encrypt their Web databases, mistakenly believing that this protects the data.

The only truly safe solution is both simple and bulletproof: Don't store credit card numbers at all. Use donation processing tools that authorize credit cards in real time and then discard the card number. Such tools process follow-up transactions, including refunds or monthly donations, using one-time reference codes that are tied to the nonprofit's account and useless to a fraudster. Card numbers are stored only by the payment gateway (the system that manages transactions and connects the Internet to banking networks), whose systems are highly secure.

Be Alert to Carding.

A practice known as "carding" is a major concern for nonprofits. Fraudsters use a low-dollar online donation to test the validity of guessed or stolen card numbers. Although carding doesn't defraud the nonprofit, the organization is burdened by the administrative work required to issue a refund to the real credit card holder. Until recently, the only solution was for an organization to use software that monitored the Web site for failed transactions. Today, however, use of additional CVV2 security codes (the 3-4 digit additional numbers on credit cards) is a promising alternative. Unlike the old Address Verification System (AVS), CVV2 was designed for automated fraud protection, and is gaining ground in the United States.

Don't Put Your Online Donors at Risk.

Strict credit card security is critical for any organization accepting online donations on its Web site. By keeping in mind key issues when creating security strategies, you can help ensure safe transactions for your online donors. ■

The only truly safe solution is both simple and bulletproof: Don't store credit card numbers at all.

Resources

Allen, Nick, "Using E-Mail & the Web to Acquire & Cultivate Donors," *Nonprofit World*, Vol. 21, No. 1.

Bhagat, Vinay, "Leveraging Your Web Site for High-Impact Marketing," *Nonprofit World*, Vol. 23, No. 5.

Crooke, David, "E-Mail Deliverability: Increase Your Chances of E-Mail Getting Through," *Nonprofit World*, Vol. 23, No. 2.

These resources are available free at www.snpo.org/members.

David Crooke is the co-founder and chief technology officer for Convio, Inc. (www.convio.com), a leading provider of software and services to help nonprofit organizations use the Internet to become more effective at fundraising, mobilizing support, and managing constituent relationships.

Nonprofit World • Volume 25, Number 2 March/April 2007
Published by the Society for Nonprofit Organizations
5820 Canton Center Road, Suite 165, Canton, Michigan 48187
734-451-3582 • www.snpo.org

Advertiser's Index