



A Secure Website is Essential to Customer Trust

BY DOUG BEATTIE

When it comes to online shopping, consumers spend close to \$6 billion each year. This growing number presents a significant opportunity to small businesses but without a secure website, consumers may not feel comfortable enough to shop or complete a transaction. To solidify a trusting relationship with customers and drive online sales, small businesses must prioritize online security in five ways.

1. Verify your company's identity with an SSL certificate. SSL technology is an important part of building trust among online shoppers. With SSL, your website's URL includes a padlock symbol and begins with "https" instead of "http," both of which are signs of a secure website. According to a survey from the CA Security Council, more than half of consumers recognize and look for the padlock symbol, meaning that an SSL certificate could make the difference in whether customers choose to make a purchase on your website.


2. Consider upgrading to EV SSL technology. An EV (Extended Validation) SSL certificate takes SSL a step further by providing the highest degree of authentication. In addition to "https" and the padlock symbol, your website will display your company's name in green on the browser address bar, an additional sign of security understood by 42 percent of consumers according to the same survey. Consumers know to look for the green bar and padlock before trusting a website with their information.

3. Keep track of your website's account information. When hiring an outside entity to build their websites, many business owners leave that individual as the only one with the account information for the SSL certificate, hosting account, and domain name. This causes a problem when the business owners need to change or

renew the accounts. Instead, small businesses should maintain access to their usernames and passwords so that they can manage all aspects of their websites.

4. Use effective passwords that are difficult to break. All passwords should be longer than seven characters and include numbers and special characters. Programs can allow attackers to easily guess your passwords and threaten the security of your website. To help prevent this, use password safes, password generators, and two-factor authentication whenever possible. By using these precautions, your company's website will be a secure and safe place for customers to shop.

5. Install security updates and scan for malware. Websites are a target for malware and other threats which can lead to slow loading and unwanted ads. Malware can even spread from your website to customers' computers and smartphones, threatening the trust and relationships you have built with those customers. On a regular basis, scan your website for malware and install all necessary patches and updates. Consider installing a security program that runs these scans automatically.

Consumers understand the basics of online security and know to avoid websites that may put their financial information in jeopardy. This highlights the need for small businesses to put their customers first and make sure these security measures are in place. By offering the highest level of security, small businesses communicate their trustworthiness and a strong commitment to protecting their customers. 

Doug Beattie is the Vice President of Product Management at GMO GlobalSign and the Steering Committee Member at the CA Security Council. You can reach Doug by email at douglas.beattie@globalsign.com, by phone at 617-645-3675, or visit his websites at www.globalsign.com/en/ and www.cosecurity.org.