Securing Your Small Business Online

Intro: Small Business, Big Threat
Get World-Class Security with SSL
Give Customers the Green Light
Throw Hackers a Curveball with ECC
Assure End-to-End Security with Always-On SSL
No One’s Perfect—but You Can Be Close
Symantec for Your Small Business
Securing Your Small Business Online

Small Business, Big Threat

Hackers are taking aim at your small business website. Defend yourself—and your customers—with strong, affordable online security.

Years ago, a small business could attract customers online with low prices alone. No longer. Consumers these days are well aware that cyberfraud is a serious danger, and they won’t do business with you online unless they’re sure your website is secure. That means you must do two things: One, secure your website. Two, assure visitors to your site that they’re protected while they’re there.

Yet a lot of businesses do neither. Many think hackers don’t bother with small businesses. Not true. The January 2014 Symantec Intelligence Report shows companies with fewer than 250 employees are the victim of 39 percent of all cyberattacks. Others think they can’t afford strong security. Again, not true. Small businesses today can get the same protection used by large companies—and get it at an affordable price. These security solutions are easy to implement and easy to manage, with no need for onsite IT staff.

The small-business takeaway: Now is the time to secure your website, instill confidence among your customers, and reach your full potential online.

View the infographic below to learn why small business is a big target for cybercrime.

Consumers these days won’t do business with you online unless they’re sure your website is secure.
Securing Your Small Business Online

Get World-Class Security with SSL

From Wall Street to the megamall, high-profile cyberattacks are making headlines on a regular basis. Identities are stolen, accounts intercepted, credit card numbers swiped. It’s enough to make people worry about their security at the websites of the nation’s largest retail and financial institutions. So what do you think it does to consumer confidence in your small-business site?

To assure your customers that your website is safe, you must secure your site and you must implement a solution that’s recognized and trusted by consumers. Your best choice: SSL, or secure sockets layer protection. The world’s largest companies use SSL security to safeguard their websites. In fact, 91 percent of Fortune 500 companies use Symantec SSL—and the same product is available to your small business.

Click on the article below to read frequently asked questions about SSL security for your small business.

Q&A What's the Best Way to Protect My Small Business Website?

Give Customers the Green Light

You not only must protect your customers when they visit your site, you must make it apparent to them that they’re protected so they’ll feel safe enough to do business with you. A good way to do it is with Symantec Extended Validation SSL Certificates.

For you, Symantec EV SSL means strong website security. For your customers, it means the address bar in their web browser turns green when they visit your website, a clear signal that your site is legitimate and trustworthy. And more trust among your customers means more sales conversions for your business. Websites that use Symantec EV SSL have an average of 17 percent uplift in sales-conversion rates.

Learn how these three small businesses boosted their trust—and their sales—with the green bar.

Read the article below to learn how a simple signal that your site is secure can instantly boost your bottom line.

CASE STUDY Green Means Go

Q&A What’s the Best Way to Protect My Website?
Throw Hackers a Curveball with ECC

Cyberattacks are coming fast and from many directions. And for small businesses, the repercussions are usually catastrophic.

Without the resources to repair the damage done by a breach, most small firms never recover. In fact, 60 percent of small firms that fall prey to cybercrime go out of business within six months of the attack, according to the National Cyber Security Alliance.

You can fight back with ECC, or elliptic curve cryptography. ECC is one of the most powerful and efficient types of encryption available today. ECC is the next generation of encryption algorithm. It offers stronger security than certificates that use the 2048-bit RSA algorithm and it’s 10,000 times harder to crack. It’s also more efficient, and becomes even more so under peak server loads.

To demonstrate the power of ECC, Symantec includes an ECC certificate with our Symantec Pro SSL products, ensuring that you’ll always have the latest technology when you upgrade to Pro. Symantec is also the only company to offer pure ECC certificates—ECC certificates chained to ECC roots. The only other company to offer ECC certificates chains them to RSA certificates, which provides less than ideal security.

Visit the article below to read five reasons why you may need the enhanced capabilities of ECC.

60 percent of small firms that fall prey to cybercrime go out of business within six months of the attack.
Securing Your Small Business Online

Assure End-to-End Security with Always-On SSL

Small businesses routinely use more secure SSL to protect login pages and shopping carts. But many stop there. They don’t encrypt subsequent pages during the user’s session. Once upon a time, that may have been enough. But nowadays, when online attacks are frequent and easier to execute, you must ensure that all online transactions involving confidential data are locked down all the time.

Always-On SSL does that. It enforces the stronger security of SSL across your entire website. With consumers now well aware of the risks posed by cybercrime and data loss, they look for proof that the companies they transact with are taking serious measures to protect them. You can address their concerns—and yours—with Always-On SSL. Top websites like Apple and Amazon use Always-On SSL in their strategy to deliver a better shopping experience to their customers. You can do the same.

Click on the article below to learn how Always-On SSL protects users with persistent security from login to logout.

Top websites like Apple and Amazon use Always-On SSL in their strategy to deliver a better shopping experience to their customers. You can do the same.
No One’s Perfect— But You Can Be Close

Secure once meant, well, secure. It meant that pages transmitted via HTTPS (the “S” stands for secure) rather than HTTP were protected from prying spies. Then the Heartbleed bug changed everything. Its discovery revealed that HTTPS sessions based on one specific version of Open SSL are indeed vulnerable to attack if a hacker can learn a server’s private key. If he does, he can read any information sent to the server.

Perfect Forward Secrecy can stop the bleeding. It provides an added layer of security not available with common Open SSL products. It protects you even if an eavesdropper does gain access to your server’s private key. Perfect Forward Secrecy can be more costly. But, as the Heartbleed bug demonstrated, the cost of not running PFS can be far greater.

Symantec offers a free tool you can use to check your security and make sure your certificate is installed correctly and employs the latest protection. To check your certificate, go to https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp.

Read the article below to discover how perfect forward secrecy provides better protection for your website.

Symantec’s innovative products and services protect businesses small and large. Our world-renowned expertise in safeguarding data, identities, and interactions delivers security and confidence to you and your customers.

To learn more about strong, affordable online security for your small business, visit us at Symantec.com/ssl-certificates.