Built on Trust
A Guide to Creating a Secure and Successful E-Commerce Business
It's easy to see why e-commerce is so popular. Shopping online is quick and convenient, and consumers can purchase nearly anything from nearly anywhere in the world. Retail e-commerce sales—which include products and services (barring travel, restaurant and event ticket sales) ordered via the internet over any device—will reach $1.92 trillion in 2016, accounting for 8.7 percent of total retail spending worldwide. While the pace of growth for overall retail sales is subdued, the digital portion of sales continues to expand rapidly, with a 23.7 percent growth rate forecast for 2016.¹

The internet economy is one of the best things to happen to both consumers and merchants. Although the online economy is ripe with opportunity, it's also full of potential pitfalls that can trap even the savviest businessperson, so there are some important things you should know before diving into e-commerce.

In this guide, you will learn the basics of setting up your e-commerce site and selecting the right security measures to help you gain the most customers.

Don't Know How to Code? Don't Worry.

You have the perfect idea for an e-commerce business. Maybe you've invented the next must-have gadget, or perhaps you perform a unique service that no one else in your area offers. Whatever your idea may be, you need a website. But you don't need to be an expert programmer or HTML guru to get your site up and running. You just need to find the right web design option to meet your needs.

There are many web design companies that specialize in building e-commerce sites. There are also companies that offer do-it-yourself options, which include tools to easily select all of the features you want on your site without enlisting outside help. But before you contact a design company or start building your own site, do a little research.

Retail e-commerce sales will reach $1.92 trillion in 2016, accounting for 8.7% of total retail spending worldwide.¹

Having a clear vision of what you want your site to look like and how it should function will make the process much easier. Consider making a list of your favorite online stores and jot down some notes about each one.

Some questions you might ask yourself include:

- What do I like about these sites?
- Are the sites easy to navigate?
- What features/elements do they have that appeal to me?

Next, contact the companies that made some of your favorite sites or peruse the web for build-it-yourself services you can use to create your own site. The benefit of building your own site is that you can quickly get your business up and running without much cost and update it yourself as your business changes. Paying a designer to create your site will be pricey and take a bit longer, but in the long run it may be worth the expense. You'll get the exact features and look you're after, and you'll have a web expert to update your site's programming as your business grows.
Gain the Trust You Need

Your new e-commerce site may look good and offer all the features you hoped for, but it can't get off the ground if your customers don't trust it. E-commerce is risky business—and online shoppers are concerned about fraud. In fact, a recent poll found that 18 percent of e-commerce sites had shopping cart abandonment due to security concerns.\(^2\)

Before your potential customers click the **Buy** button, they'll want to feel secure that your site is legitimate and that their personal and financial data will be protected during transactions. That's why all e-commerce sites need **Transport Layer Security (TLS)** or **Secure Sockets Layer (SSL)** security certificates and site verification.

**SSL/TLS Certificate Basics**

SSL/TLS certificates are small chunks of code that are installed on e-commerce sites. When a user clicks the **Buy** button to place an order on a secured site, the SSL/TLS certificate scrambles, or encrypts, the user's financial information before it is transmitted online. If the information is intercepted by cyber criminals, the SSL/TLS certificate makes sure that it cannot be deciphered. Without SSL/TLS security, customers' personal and financial data is free to any hacker who can catch it as it flows over the internet.

But there's more to SSL/TLS certificates than just the code and encryption. Companies that provide SSL/TLS certificates, known as certificate authorities (CAs), also perform site verification. Verification is the process of confirming that e-commerce sites are legitimate businesses and not scams set up to collect confidential information from unsuspecting users.

When verifying a site, CAs like Symantec contact website owners and request documentation to establish company ownership and credibility. Each CA uses different steps and procedures to obtain this information, but Symantec offers a fast, simple process that makes it easy for website owners to get a new SSL/TLS certificate in a matter of days.

When you're developing your site and considering your options, working with providers that offer credible SSL/TLS certificates should be one of your top concerns. For example, if you decide to use a fully hosted third-party e-commerce platform, then you need to make sure that the provider supports SSL/TLS certificates from a well-known, reliable CA like Symantec.

If you don't vet the providers you work with thoroughly, it may come back to haunt you. Even though e-commerce platform solutions will be technically responsible for securing your transactions, customers will most likely hold you partially responsible if their personal information is stolen.

Working with providers that offer credible SSL/TLS certificates should be one of your top concerns.
Signs of Safety

It's easy to tell if a site is using SSL/TLS certificates, but only if you know exactly what signs to look for. First, the site's web address will start with “https” instead of “http.” The “s” you see lets you know the site is secured and the information provided on this site will be encrypted. Secondly, popular web browsers like Chrome, Internet Explorer, Firefox and Safari will display a padlock icon, usually next to the website’s address. Clicking on the padlock will display information about the certificate, including which CA issued it and which company owns it.

In newer releases of Chrome, Google has begun inserting an exclamation point inside of a circle in the address bar on non-secure sites. This is just the first step in a series of changes that will eventually include additional negative visual indicators Chrome will use to mark unencrypted websites. For example, in upcoming versions of Google Chrome, the company will add the words “Not secure” next to the exclamation point icon for sites that are not encrypted.

Build Customer Confidence with Trust Marks

When a business purchases an SSL/TLS certificate, some CAs, including Symantec, will also provide a small image that the company can display on its website. These images, called trust marks or trust seals, make it even easier for visitors to see that a website is authentic and safe. The most useful trust marks are dynamic, allowing visitors to click on them and get up-to-the-minute information about a site’s security status.

For example, the Norton™ Secured Seal displays information about the kind of SSL/TLS certificate a site uses, the domain the certificate is issued to and when the site verification expires.

A trust mark will only do its job if website visitors can see it. That's why it's important to make sure that your trust mark is displayed prominently on your site. Placing the image near the top of your home page will immediately show visitors that your site is secure. You should also consider putting the trust mark in your website’s footer. That way, the seal will be part of your company’s identity no matter what page customers visit.

Also, a trust mark on product or checkout pages directly next to Buy Now or Place Order buttons can make customers feel comfortable enough to complete a purchase. Norton Shopping Guarantee can do all of these things and more by offering key trust-inviting features like identity theft protection, a purchase guarantee and pricing guarantees. Businesses that use the Norton Shopping Guarantee have also been shown to boost conversion rates by an average of 7 percent, and customers return to shop more often to sites with the Norton Shopping Guarantee.³
Get the Right Kind of Validation

Because CAs are responsible for verifying sites, choosing a credible SSL/TLS provider is critical to your company’s success. When choosing an SSL/TLS provider, stick with a company that has a long history of providing security to successful e-commerce sites. Savvy internet shoppers will look for familiar security brands like Symantec, the most recognized trust mark on the internet.

Every business is different. Given that, there are three types of SSL/TLS authentication: Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV). Each of these types of validation offers a different level of verification that a business or entity is legitimate and thus offers a different level of potential trust from your customers.

**Domain-validated** SSL/TLS delivers encryption and authentication that confirms that the person applying for the certificate has the right to use a specific domain name. DV certificates are most appropriate for internal server applications since they don’t provide significant assurance to help your customers trust you.

**Organization-validated** SSL/TLS comes with the necessary “https” label, plus authentication that the company or organization claiming the website is a confirmed legal entity and a physical location for that entity has been confirmed. If a website visitor clicks on this type of certificate, they will find information on the company or organization sponsoring the website.

Unfortunately, hackers have tried to trick the system by issuing their own SSL/TLS certificates and fabricating site verification information. That’s why a group called the CA/Browser Forum developed guidelines for Extended Validation (EV) SSL/TLS Certificates in 2007—making EV the strongest, safest option for SSL/TLS security. When a site uses EV SSL/TLS, the company must undergo a more thorough verification process to confirm the identity of the business.

**Extended Validation** is ideal for e-commerce sites that process credit card transactions. Not only does EV deliver all the functions of an OV certificate, it also triggers highly visible security indicators in the browser of your website visitors. Namely, in high-security browsers, the bar displays the name of your organization and the certificate authority who issued your SSL/TLS. You can get these features with a Symantec EV certificate. Many web businesses have reported a noticeable increase in completed transactions as a result of implementing an Extended Validation SSL certificate.

Depending on the type of business validation required by the CA, receiving your SSL/TLS certificate can take anywhere from a few minutes to a few days. Even though the different levels of validation may seem complicated, SSL/TLS providers like Symantec make the process of obtaining an SSL/TLS certificate easy and straightforward.

**Success Within Reach**

Building and securing an e-commerce site can be a lot of work, but the rewards can be tremendous. In the online marketplace, a startup can turn into an international sensation overnight, especially when it has a site customers can trust.

But big-time success only comes with proper planning and execution. Build a clean, easy-to-use site, secure and authenticate it with a credible SSL/TLS provider like Symantec, and protect it with tools that have a proven track record for instilling the most customer trust. If you follow these simple rules of thumb, your site will be well on its way to success.

To learn more, contact our sales advisors:

- **Via phone**
  U.S. toll-free: 1-866-893-6565

- **Visit our website at**
  www.symantec.com/ssl

---

1 https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369#sthash.Y0A3LqAX.dpuf
2 http://baymard.com/lists/cart-abandonment-rate
3 https://www.nortonshoppingguarantee.com/merchants/
For global offices and contact numbers, please visit our website.

For product information in the U.S., call: 1-866-893-6565 or 1-520-477-3111

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/ssl

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Website Security Solutions Pty Ltd:
3/437 St Kilda Road, Melbourne, 3004
ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

Follow Us:

For product information in the Americas (Non-U.S.), call:
Mexico: 554 738 0448
Brazil: 800 038 0598

For product information in the U.K., call:
0800 032 2101 or +44 (0) 208 6000 740

Symantec (UK) Limited.
350 Brook Drive
Green Park, Reading
Berkshire, RG2 6UH UK
www.symantec.co.uk/ssl

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929
Germany: 0800 128 1000
France: 0800 90 43 51
Spain: 900 93 1298