Gaining Customer Confidence with Extended Validation (EV) Certificates

digicert®

Table of Contents

digicert®

Introduction

As e-commerce expands, customer trust is essential to financial success, customer conversion, and business growth. However, cybercriminals have become adept at fooling customers into thinking they're visiting a legitimate website by using visual cues similar to real online trust markers.

Customers need to be reassured that their confidential information is safe and protected from malicious activity. Without concrete proof that their data is protected, customers may abandon their shopping cart when prompted to enter sensitive information. DigiCert EV SSL Certificates are specifically targeted at increasing customer confidence in e-commerce through specific, EV certificate-only browser cues.

In this article you'll learn (1) how prevalent cybercrime is and why online consumers should be cautious, (2) how Extended Validation (EV) certificates differ from basic SSL certificates, and (3) why you should consider using an EV certificate.

Current State of Web Commerce

As access to the Internet grows, more people are spending time online than ever before. Industry experts predict online accounts will become the primary customer touchpoint within a decade. However, many people are still reluctant to conduct transactions online due to concerns about protecting financial information and increasing consumer awareness of online scams. The financial consequences of this reluctance are easy to measure:

- Shopping carts are abandoned, causing a loss in sales and revenue
- Click-through tracking shows that potential customers reach enrollment forms but don't fill them out
- Search analytics show that brands and company names are often hijacked to lure customers away from legitimate sites

Internet scams have become more coordinated and sophisticated, eroding the consumer trust essential to online business. Across 2015 and through the first half of 2016, phishers targeted between 393 and 442 unique brands in any given month. In Q2 of 2016, The total number of unique phishing sites observed was 466,065. This was 61% higher than the previous quarterly record in Q4, 2015. These trends have contributed to the fact that 70% of all online shopping carts are abandoned (up from 60% a decade ago).

Cart Abandonment and Recapture Statistics

2016 State of eCommerce

on average

68.63%

of shopping carts abandoned

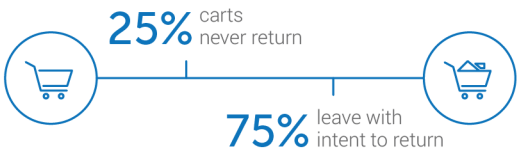
estimated value of

4.9 trillion

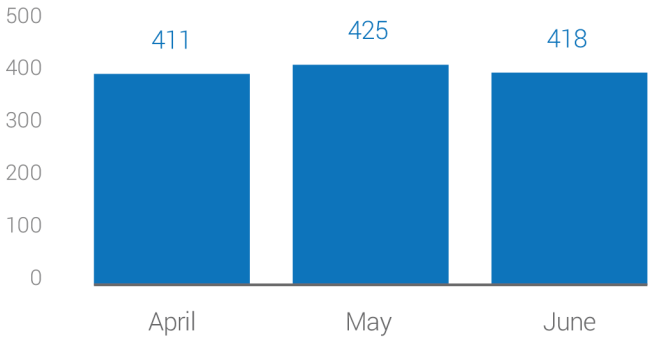
abandoned carts globally

99%

of people won't' buy on first visit



Hijacked Brands, April - June 2016



digicert®

History of SSL Certificates

Most websites use SSL Certificates to encrypt data and assure their visitors they've reached an authentic site. SSL (Secure Sockets Layer) is a security technology that was invented to establish an encrypted link between a server and a client—typically a web server (website) and browser, or a mail server and mail client (e.g., Outlook). SSL allows sensitive information (credit card numbers, social security numbers, login credentials, etc.) to be transmitted securely. The third party vendors that issue SSL Certificates are called Certificate Authorities, or CAs.

The creation of the SSL protocol provided consumers with a much needed boost in confidence and trust in e-commerce and the online experience in general. But as the threat of phishing and pharming grow each day, online trust has eroded significantly.

In response to these sophisticated exploits, DigiCert and other leading CAs came together with browser providers like Microsoft and Mozilla to form the CA/B Forum. Their objective was to develop guidelines to improve how SSL worked, along with the associated validation process. The creation of Extended Validation or EV SSL Certificates was the first result of that effort. EV SSL Certificates undergo a more rigorous validation process, and subsequently display special EV certificate-only browser cues. EV SSL Certificates not only create an encrypted connection between a server and a browser, but verify that a trusted third party (the CA) has authenticated that organization's identity.

What is an Extended Validation (EV) Certificate?

EV certificates are SSL Certificates that require a detailed and rigorous validation process. Any CA offering EV certificates must comply with a strict, security-minded validation process. This process includes verifying that the requestor has:

- Legal rights to use the domain
- Properly authorized the issuance of the certificate
- Legal status and physically exists
- An identity that matches official records

During this process, a representative from the CA will contact the requester at a verified phone number to confirm they requested the certificate and are authorized to receive it. Maintaining this human element in the process provides an additional layer of defense against fraudulent or phishing-related activity.

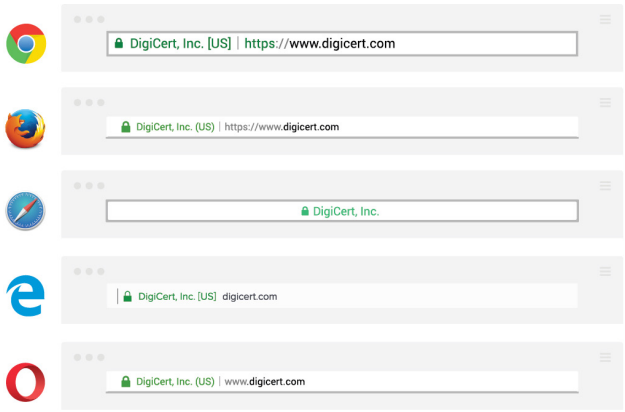
To notify the user of an EV certificate on a website, browsers show specific visual cues:

- Green in the address bar
- Company name and padlock in the address bar
- https:// at the beginning of the address
- Company information in the certificate details

How Do EV Certificates Increase Customer Confidence?

As detailed above, customer confidence in e-commerce decreases when users can't tell the difference between real business and phony phishing websites. High-profile incidents of fraud and phishing scams have made users more concerned about protecting their information online—they may abandon their shopping cart or other transactions when prompted to enter sensitive information. Because of the additional visual cues EV certificates provide, users are assured they're on an authentic and validated website.

That said, these visual cues are only as strong as what they represent. Users can trust the browser cues of an EV certificate because the verification process is so rigorous. As EV certificates become more prevalent, users will begin to look for and trust the green bar. (This is illustrated in the graphic below.)



Why Should I Buy an EV Certificate?

An EV certificate lets your visitors complete secure transactions with confidence, decreasing cart abandonment rates. An EV certificate also puts your organization in a leadership position. If your site has the green bar and your competitor's site does not, you have a competitive advantage by appearing more trustworthy. For businesses with a high profile brand, using EV certificates is one of the best defenses against phishing scams. When customers see the green bar and the name of your security vendor, they can interact with you online without fear and their confidence in e-commerce grows.

Why Buy an EV SSL Certificate from DigiCert?

The Certificate Authority (CA) you select will impact ease-of-use, speed of issuance, uptime, OCSP/CRL latency, and a variety of features that can make your network more secure and simple to manage. DigiCert® has been providing SSL Certificates and SSL management tools for over a decade, and assisted in developing the Extended Validation Certificate. DigiCert has an award-winning in-house technical support team and some of the fastest certificate issuance times—with EV certificates typically issued in a matter of hours!

Experience the "DigiCert difference" for yourself by calling 1.800.896.7973 or visiting digicert.com.

digicert®