White Paper

How Extended Validation SSL Brings Confidence to Online Sales and Transactions

Symantec

Norton SECURED
powered by Symantec

How Extended Validation SSL Brings Confidence to Online Sales and Transactions

CONTENTS

Introduction

As customers increasingly choose to shop, share, bank, and view accounts online, they have become more savvy about security. However, concerns about identity theft and fraud still keep many website visitors from completing, or starting, their transactions online. They need to be reassured that the confidential information that they share will be protected from malicious activity.

Symantec™ Extended Validation (EV) SSL Certificates can be a key factor in helping increase customer confidence during online business transactions. More confidence can mean more conversions for customers with EV SSL certificates. Symantec EV SSL turns address bars green in high-security browsers for an extra layer of website security that customers can see and trust.

Online Growth Slowed by Lack of Trust

Today, more people have access to the Internet and spend more time online than ever before. Financial industry experts predict that online banking, and other accounts, will become the primary customer touch-point over the next decade. As Internet adoption continues to grow and Web browsing becomes more common on mobile devices, businesses have the opportunity to tap new markets with online sales and account-based services. However, reluctance to conduct transactions online remains due to concerns about protecting confidential information. Even though identity theft occurs more often offline than online, many Internet users are nonetheless extremely wary of identity theft. On the Web, the impact of this doubt is easy to measure:

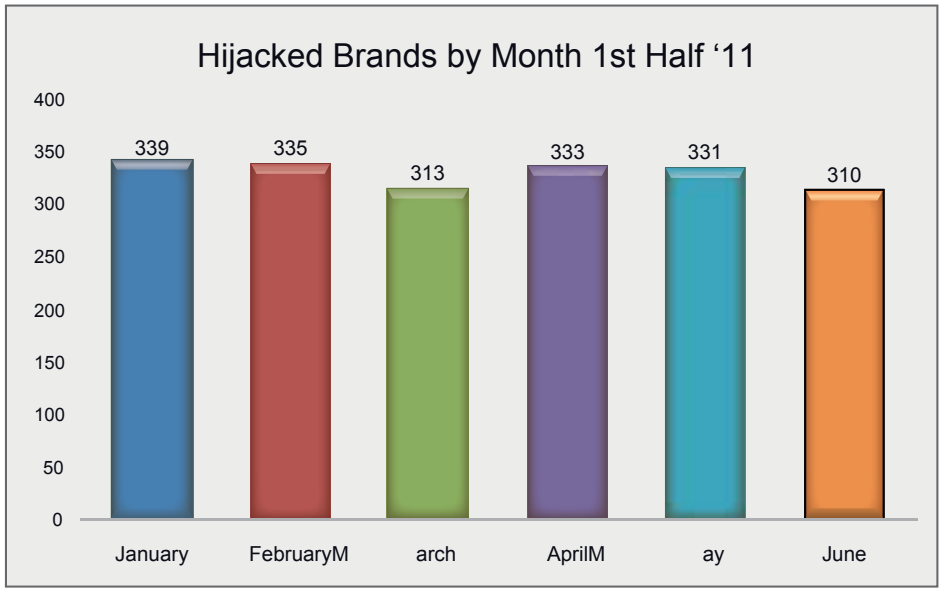
- Abandoned shopping carts add up to lost sales and missed revenue.
- Click-through tracking shows that potential customers reach enrollment forms, but do not complete them.
- Search analytics and alerts show how brands and company names are hijacked to lure customers away from legitimate sites.

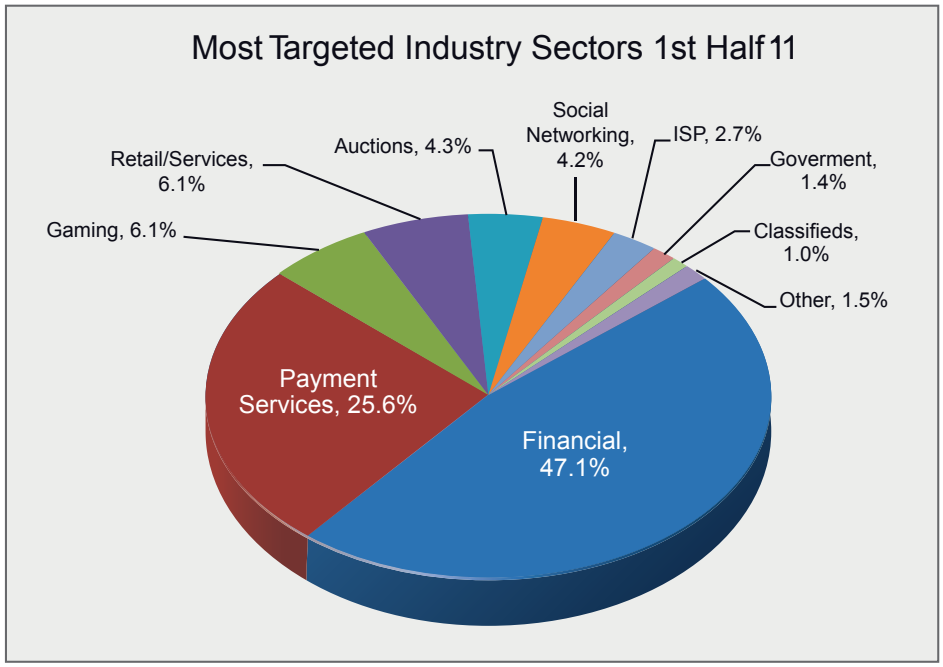
Internet scams have become more coordinated and sophisticated, eroding the trust that is essential to online business. In the second half of 2010 the Anti-Phishing Working Group reported an average of 305 brands hijacked each month, with September having the highest monthly incidence at 355.[1] Phishing schemes use emails and websites that appear legitimate to trick visitors into sharing personal information. SSL stripping, a type of man-in-the-middle attack, redirects users to “secure” websites that are fake (i.e., some security measures have been taken, and are displayed, but the website is not really the one the visitor believes they are visiting). These types of attacks often target webmail applications, secure sites, and intranets.

[1] Source: www.antiphishing.org. Anti-Phishing Working Group 2010.

Phishing Defined

A type of fraud where emails and websites that appear to be from a well-known brand are actually fake sites where information is captured and used for identity theft.





APWG,Phishing Activity Trends Report: 1st Half 2011 (2011), Page 5, http://www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf

Extended Validation Restores Confidence

Many website owners are familiar with the visual indications that a website is using SSL – the closed padlock and "https" in the URL are examples. Before Extended Validation SSL, website users had to trust that only legitimate sites were secured with SSL. Fraudsters have abused this trust by taking advantage of lax validation policies used by some Certification Authorities (CAs), and purchased SSL certificates for fake domains. They have used these SSL certificates to create "secure" sites from which to launch phishing and man-in-the-middle attacks, thereby undermining overall consumer confidence.

Symantec EV SSL Certificates address this nefarious use of SSL, and offer an easy way to help reduce abandonment and increase conversions. All accomplished while lowering costs and protecting personally identifiable information (PII) through more secure online transactions.

How Extended Validation Works

Extended validation authentication provides the highest level of authentication available with a SSL certificate. EV SSL certificates provide an extra layer of protection for consumers and website owners by requiring that applicants follow a strict issuance and management process, as defined by the CA/Browser Forum, prior to being issued an EV SSL certificate. Support for EV SSL has become a standard security feature in mainstream Web browsers such as Internet Explorer and Firefox, and on mobile devices such as the iPhone and Droid. These browsers recognize EV-secured websites and show the presence of EV in a visually distinctive way so that users can easily see that the website can be trusted. When customers visit a webpage secured with an EV SSL certificate, the address bar turns green (in high-security browsers) and a special field appears with the name of the legitimate website owner along with the name of the security provider that issued the EV SSL certificate. This visual reassurance has helped increase consumer confidence in e-commerce.

Backed by the Most Trusted Name on the Internet

EV SSL also helps users determine who they are doing business with and who validated the website. The address bar in EV SSL-compatible browsers shows the name of the organization that owns the EV SSL certificate and the SSL provider that issued it.

The Norton™ Secured Seal, is displayed over half a billion times per day on websites in 170 countries and in search results on enabled browsers as well as partner shopping sites and product review web pages. A Symantec EV SSL Certificate reinforces the notion of brand and site security by placing the trusted Norton Secured Seal with the Norton™ Check next to the website owner's company name in the address bar.

Symantec: The #1 Provider of Online Security

Symantec is the world's leading provider of SSL certificates and maintains more EV SSL certificates than any other CA[2]. Web users are accustomed to seeing commercial e-commerce websites display the Norton Secured Seal – prominently featured to assure online users that their online business is authentic and that their site is capable of securing their confidential information with SSL encryption.

Higher Authentication Standard

Before issuing an EV SSL certificate, the SSL provider must:

- Verify the legal, physical and operational existence of the entity
- Verify that the identity of the entity matches official records
- Verify that the entity has exclusive right to use the domain specified in the EV SSL certificate
- Verify that the entity has properly authorized the issuance of the EV SSL certificate

The Value of EV SSL

As EV SSL adoption spreads, the green address bar is becoming a "must have" for a wide range of industries doing business online. The ability to track impressions, clicks, and interactions make it possible to measure the return on investment in EV SSL and quantify the value of better security to any company's bottom line.

Converting browsing shoppers into buyers and visitors to members requires a high degree of trust and confidence in a given website. In industries where fraud and scams are common, the rigorous authentication process behind EV SSL sets reputable firms apart. Many companies have found that a Symantec EV SSL Certificate helps them establish their online presence, because Internet users know and trust the Symantec brand. In recent tests, 77 percent of consumers recognized the Norton Secured™ Seal, more than our competitors' trust seals[3].

Better Protection

For companies that must comply with regulatory standards related to securing personally identifiable information, EV SSL certificates help reduce risk of non-compliance and communicate the implementation of rigorous protection measures against well-known threats. By using EV SSL, and educating customers to look for the green bar, companies mitigate the risk of mid-stream interception and demonstrate efficacy of security measures.

Choosing the right SSL certificate provider is also important to getting the best possible protection. Symantec SSL Certificates secure more than one million Web servers worldwide[4]. Symantec's rigorous authentication process, audited annually by KPMG, leads the industry in reputation qualification measure to establish an online business credibility.

[2] Includes Symantec subsidiaries, affiliates, and resellers.
[3] Symantec Consumer Research Study, January 2011.
[4] Includes Symantec subsidiaries, affiliates, and resellers.

Conclusion

Online services and sales have become areas of growth for businesses of all sizes across a wide range of industries. Symantec SSL Certificates with EV are a proven tool that makes it easy for customers to feel confident about sharing their personal information online. They are a “must have” for businesses that want to maximize their online growth potential.

More Information

Visit our website

http://www.symantec.com/ssl

To speak with a Product Specialist in the U.S.

1-866-893-6565 or 1-650-426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world’s information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

UID: 062/10/13