

Realtime
publishers

"Leading the Conversation"

The Shortcut Guide™ To



**Extended
Validation SSL
Certificates**

sponsored by



Dan Sullivan

Chapter 4: User Experience	49
User Experience with Traditional SSL Certificates.....	49
Examples of SSL Visual Cues	50
Limitations of Typical SSL Browser Displays	52
User Awareness	53
Phishing Techniques	53
User Experience with Web Browsers	55
Internet Explorer 7 on Vista.....	55
Internet Explorer 7 on Windows XP.....	57
Mozilla Firefox	58
Benefits of EV SSL Certificates	59
Benefits to Browser Users	59
Benefits to Businesses.....	60
Brand Protection	60
Reduced transaction abandonment and increased customer trust.....	61
Summary	62

Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 4: User Experience

A key feature of Extended Validation SSL certificates is that they provide users with identify verification of the companies, government agencies, and organizations with which they do business. Previous chapters explained the standards EV SSL certificate holders must meet as well as the regulations governing CAs that issue EV SSL certificates. In this chapter, we turn our attention to the benefits of EV SSL certificates to users.

A key factor in ensuring the effectiveness of the Extended Validation SSL standard is that it was defined through contributions from a consortium of Certification Authorities and browser manufactures. In turn, the browser manufacturers have released or plan on releasing enhanced versions of their browsers that illustrate the unique interface conventions associated with EV SSL.

To better understand the user experience, this chapter is divided into three sections:

- User experience with SSL certificates
- Browser experience with EV SSL certificates
- Benefits of EV SSL

By beginning with an examination of traditional SSL certificates, we can examine some of the limitations that motivated the development of the EV SSL standard.

User Experience with Traditional SSL Certificates

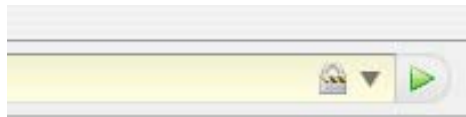
The purpose of the SSL protocol is to ensure the confidentiality and integrity of communications between a client and a server and to authenticate the server to which the client is connecting (and the client to the server if that is necessary). From a usability perspective, it is important for users to be able to distinguish encrypted communications with a trusted source from unencrypted communications with unconfirmed sources. There are, however, problems with how SSL information is displayed that limit its effectiveness.

Examples of SSL Visual Cues

Ideally, when an SSL session is established, one would have clear and distinct visual cues indicating the security status of the session. Unfortunately, the cues are not always consistent and are not as obvious as, for example, the green bar in Internet Explorer 7 when content from an EV SSL site is displayed. For example, the Internet Explorer 7 and Mozilla Firefox browsers place a padlock in the address line of a browser, as Figure 4.1 shows.



(a) Internet Explorer 7



(b) Mozilla Firefox

Figure 4.1: Visual cues of SSL status in the Internet Explorer 7 and Mozilla Firefox browsers.

This convention of a padlock on the address bar is not universally adopted, though, as illustrated by the Safari browser available for the Mac OS platform. Figure 4.2(a) shows the browser address line for a non-SSL connection while Figure 4.2(b) shows the browser address line for an SSL connection; they are the same. A user looking for a visual cue regarding the use of SSL would have to look to the corner of the browser window where a small padlock icon is displayed (Figure 4.2(c)).



(a) Non-SSL connection



(b) Address bar with SSL connection



(c) Corner of Safari window with an SSL connection

Figure 4.2: The Safari browser places the padlock icon in the address line as many other browsers do.

Limitations of Typical SSL Browser Displays

Although the padlock is a useful symbol to indicate the use of SSL, it does not provide any details about the owner of the site that is authenticated. A user might believe they are at their bank's Web site when in fact they are at a phisher's site with a URL that is deceptively similar to the real bank's Web address. To distinguish the real site from a fake site, the user would have to know enough to click on the padlock icon to reveal details of the SSL certificate (they would only see the organization's name if it is an org auth certificate). Figure 4.3 shows the details of a certificate provided by Google Mail when HTTPS is used to access the email service.



Figure 4.3: Details about the identity of the certificate owner is available by clicking on the padlock icon.

The problem with having to click through to retrieve basic identity information is that most users are not aware of this functionality; and even if they are, they may not understand the details of an SSL certificate.

This problem is not with SSL certificates per se. SSL certificates and the SSL protocol have a long and practical history. They were designed for encryption, not for conveying information about trust to a user. The advantage of EV SSL certificates is that these limitations have been overcome and in doing so avoids two widespread concerns about conventional SSL use in browsers.

User Awareness

Just as you should not have to be a mechanical engineer to drive a car, you should not have to be a security expert to effectively use authenticated, encrypted communications in a browser. There is, however, something of a gap between the top-down view of security that many users have and the bottom-up view that comes with implementing secure browsing components.

At the risk of over-generalizing, we may assume that most users have the sense that if a padlock appears in their browser window, no one can steal their credit card or other confidential information. This kind of assumption may make security professionals cringe because, depending on the type of SSL certificate used by a website, several threats exist even if the padlock is displayed:

- The site providing the SSL certificate may not actually be a legitimate business
- The site could be a phishing site posing as a well-known business site
- The site may have poor security practices leaving customer data open to theft by hackers (EV doesn't guard against this)

It is true that current SSL Certificates can ensure that data is transmitted securely (protected from third party eyes), however, there isn't a easy way to validate that the person behind the website with which you are transacting is who you intended.

Phishing Techniques

Phishers seem to have no trouble devising new ways to defraud their victims. Although the SSL protocol ensures authenticated and secure communication, it does not, by itself, ensure we can trust the other party in such a communication. Phishers take advantage of the perception of security by appearing to be legitimate when in fact they are not.

Take a simple example. A phisher registers a domain name similar to that of a well-known business, such as PayPal. The phisher registers PayPa1 (where the last character is the number one, not the letter L). Next, the phisher contacts a CA providing domain-validated certificates and receives an SSL certificate. The phisher uses the SSL certificate with the fraudulent Web site, downloads some HTML code from the real PayPal site, and in very little time can establish a site that looks legitimate. Most importantly, when users visit this site, a padlock is displayed in the browser. Phishers are taking advantage of the fact that users cannot distinguish a certificate that requires low levels of authentication with others that actually verify the identity and business viability of certificate applicants.



Domain certificates are useful to many who host Web sites. The problem with their use in phishing is that users assume a domain certificate implies that a third party is validating whether the site is safe and trustworthy. EV SSL certificates are the certificate type with the most stringent authentication standards and should therefore be the ones used when establishing trust with a customer is necessary.

Sometimes a simple copy-cat site is not sufficient to defraud a user. In such cases, phishers may resort to a man-in-the-middle attack in which they intercept traffic between a user and a legitimate site and pass the information to the legitimate site in order to generate appropriate output for the user.

Consider an example. A user receives an email asking the reader to verify account information at her bank. The unsuspecting user clicks a link in the email and is taken to what appears to be the bank's Web site. Before allowing the user to actually access her account, the bank site displays an image, selected by the user at some time in the past, and asks the user to verify that the image is in fact the one she picked. Unless a phisher has compromised the bank's authentication system, the phisher is not likely to have access to the victim's selected image. The phisher is stuck? Not necessarily.

The phisher could establish a site that has the same login page as the bank. From this fraudulent site, the phisher can collect a username and password. Then the phisher opens a connection from this site to the real bank site using the victim's credentials. The bank's Web site responds with a page that includes the user's image. The phisher replies to the user with the contents of the page generated by the bank. The victim acknowledges the correct image and the phisher does as well, resulting in an open session to the victim's account.

It sounds so easy to defeat this system, spawning the question, Why didn't the user realize the scam? Here are some of the reasons:

- The phisher used HTML code and images from the legitimate Web site. Getting this information is as simple as viewing and saving source code for a Web page.
- The initial email, called the phishing lure, was well crafted and convincing enough to ensnare the victim
- Once the user visited the fraudulent site, there were no clear indications that this was not a legitimate site.

It is unlikely that any time soon we will have a comprehensive way to address the first two issues. We can address the third reason today and, fortunately, we only need to disrupt the scam at one point to prevent a user from becoming a victim.

Traditional SSL certificates and metaphors, such as padlocks, have not been sufficient methods for controlling phishing and other forms of fraud. We will now shift attention to the user experience with browsers that use distinctive visual cues for EV SSL enabled sites.

User Experience with Web Browsers

Browsers are the most popular interface for the Internet and it is here where the added security benefits of EV SSL certificates must surface. Sites deploying EV SSL certificates have undergone a more rigorous authentication process than non-EV SSL sites and users should know this. Fortunately, new high security browsers clearly distinguish EV SSL-certified sites from others.

This section provides a series of examples of EV SSL visual metaphors and information displays from many of the most commonly used browsers, including:

- Microsoft Internet Explorer
- Opera Browser
- Mozilla Firefox, with a user add-on

This section also highlights some minor, but important, implementation issues that users should be aware of.

Internet Explorer 7 on Vista

Microsoft Internet Explorer 7 provides native support for EV SSL certificates. There are two differences that are immediately apparent with EV SSL-enabled sites. First, as one can clearly see in Figure 4.4, the Web address bar is displayed in green, indicating the use of an EV SSL certificate. More importantly from a users perspective, the green bar will likely become associated with sites that are considered more trustworthy because of the additional verification required to obtain the green bar status.

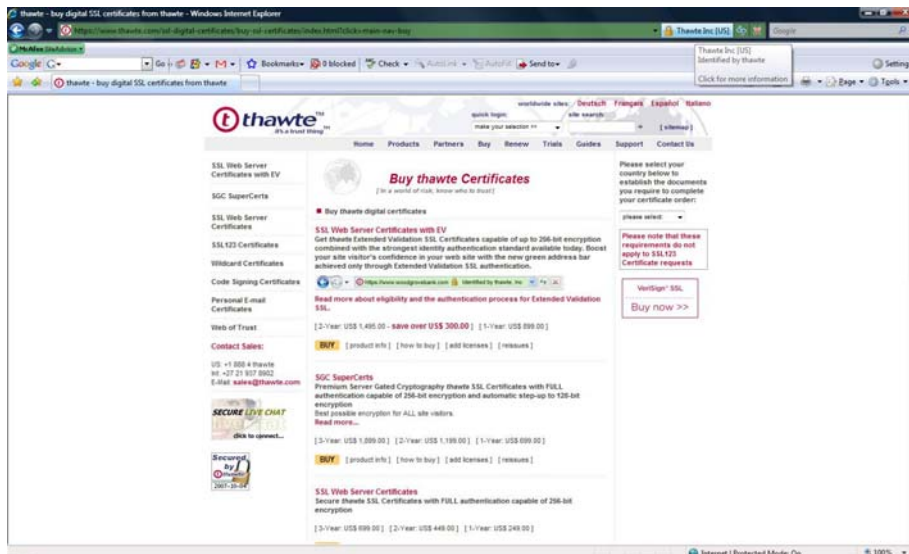


Figure 4.4: Internet Explorer 7 on Vista displaying a page from an EV SSL-enabled site.

Another visual cue provided in Internet Explorer 7, and other supporting browsers, is the name of the company or organization listed in the EV SSL certificate, which is displayed near the Web address. This is useful because regardless of what the URL looks like, a user will know the name of the organization that owns the site. A phisher may be able to secure a domain with a name similar to a well-know business, for example “bankofamericas.com.” If by some unlikely chance the phisher then obtains an EV SSL certificate for the site and has the Web address appear with the green bar, the browser will display the name on the certificate *not* the name of the legitimate business, in this example “Bank of America.”

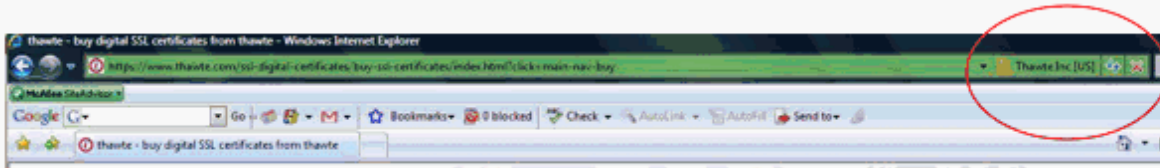


Figure 4.5: The name of the organization that was issued the certificate appears in the browser; this makes attacks using URLs similar to legitimate sites less likely to succeed.

In addition to the details that appear on the address bar of the browser, more information is available by clicking on the organization name. Figure 4.6 shows the summary information about the company in a pop-up.

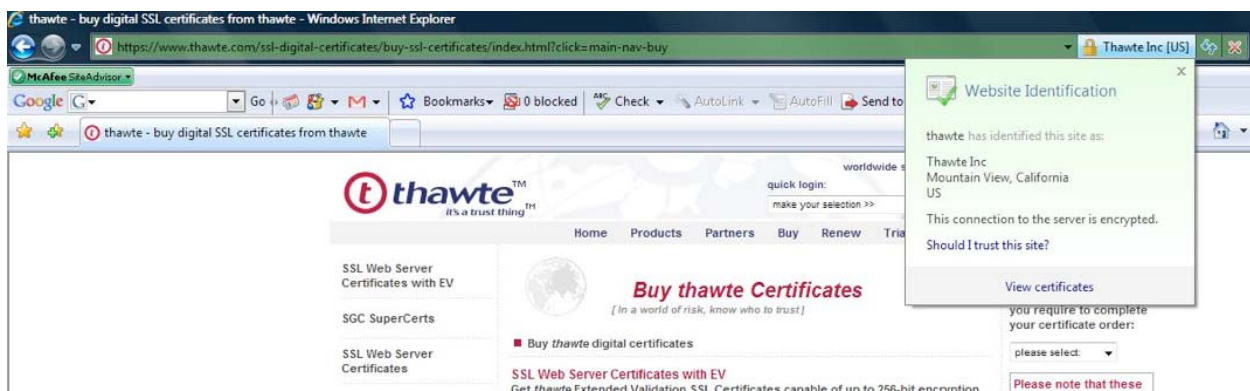


Figure 4.6: Clicking the company name in the address bar displays a pop-up box with summary information about the organization holding the certificate.

For even more information, including details about the encryption algorithm and key length, the user can click the padlock to see certificate details, as in Figure 4.7.

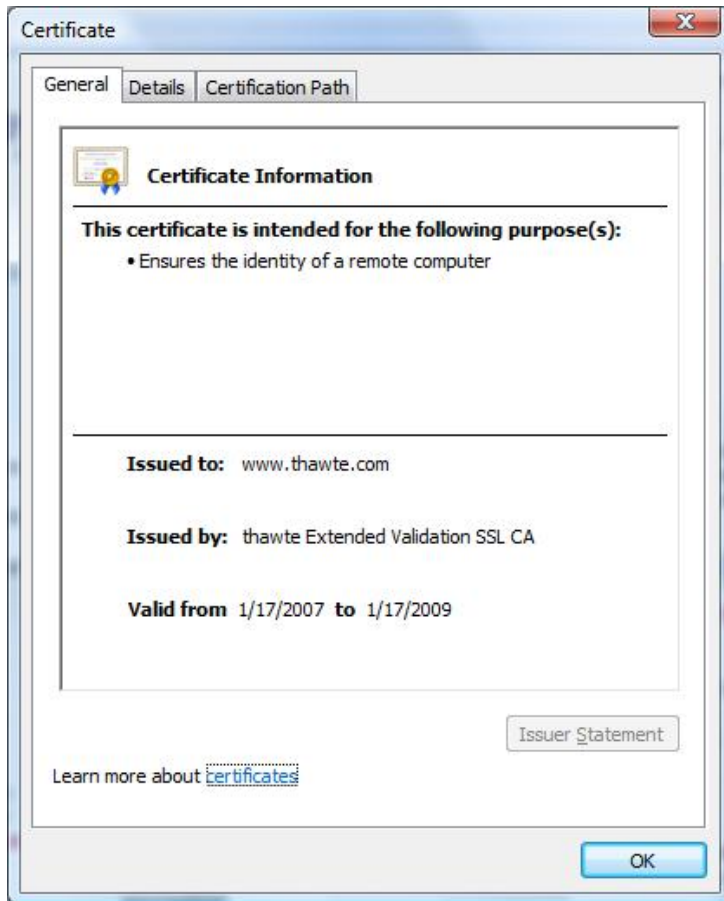



Figure 4.7: “View Certificate” displays certificate details.


Internet Explorer 7 on Windows XP

Internet Explorer 7 on Windows XP works slightly differently than on Windows Vista. Users have the same functionality described earlier but there is a difference with how Windows XP updates root certificates. Windows Vista updates its root certificates on a regular schedule. This ensures that Vista clients will have the latest certificates from CAs. Windows XP, however, only updates certificates on demand, typically when a root certificate for a CA referenced in a Web site is not currently installed. (Windows XP was developed before the EV SSL Certificate standard). To work around this problem, some CAs provide code to their customers to install on their EV certificate-enabled sites.

 Microsoft Internet Explorer 7 is available for download at <http://www.microsoft.com/windows/downloads/ie/getitnow.msp>.


Mozilla Firefox

Mozilla Firefox is another popular browser that runs on Windows, Mac OS X, and Linux. It is available in more than 40 languages. Mozilla Firefox version 3.0 will include native support for EV SSL certificates. Versions 1.5 and 2.0 of Mozilla Firefox can, however, provide EV SSL support with the use of an add-on developed by VeriSign.

 To review the status of Mozilla Firefox 3, see the project Wiki at <http://wiki.mozilla.org/Firefox3>.

The add-on is available free of charge and provides similar functionality that a user would find when using Internet Explorer 7, including:

- Recognizing EV SSL certificates issued by VeriSign, *thawte*, and GeoTrust. EV certificates from other vendors are not recognized by the add-on.
- Turns the address bar green when viewing a site with an EV certificate.
- Displays certificate owner information in the address bar
- Displays additional certificate information when the padlock is clicked.

 VeriSign EV Green Bar Extension is available for download at <https://addons.mozilla.org/en-US/firefox/addon/4828>.

When the add-on is installed, the installer notifies users that behavior of the browser will change (see Figure 4.8).

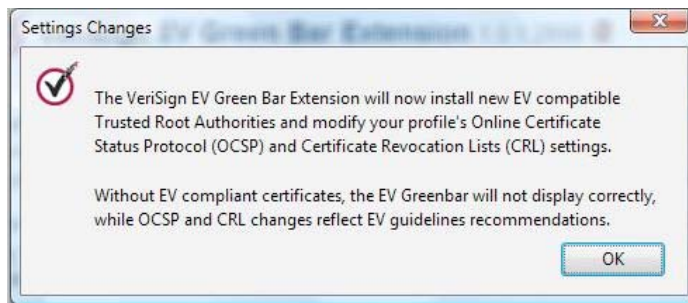



Figure 4.8: The VeriSign EV Green Bar Extension is needed with Mozilla Firefox versions 1.5 and 2.0 to support EV certificates.

The add-on works with Mozilla Firefox versions 1.5 and 2.0.

 The Mozilla Firefox browser is available for download at <http://www.mozilla.com/firefox/>.

A user's browser experience with EV SSL certificates is significantly different from other SSL certificates. Visual cues, such as a green address bar, and additional information, including the name of the certificate owner clearly displayed in the address bar provide immediate and easy-to-understand information about the trustworthiness of a site. This has clear benefits for both the user and for businesses deploying EV SSL certificates.

Benefits of EV SSL Certificates


EV SSL certificates contribute to the trust that customers have with businesses when conducting transactions online. The benefits are clearly mutual.

Benefits to Browser Users

Conducting commerce over the Internet greatly expands the opportunities for customers. They are no longer constrained by geography to shopping or doing business with nearby establishments. Concerns about phishing and identity theft leave consumers wondering, who can be trusted? The introduction of EV SSL certificates can help mitigate these concerns as recent research shows.

A study, undertaken by Tec-Ed, Inc. on behalf of VeriSign, measured the consumer expectations and responses to EV certificates and the associated browser support. The research found:

- The vast majority of users, 93%, preferred to shop with sites that displayed the green bar address line.
- Only 63% percent of shoppers would provide credit card information to non-EV certificate sites, but 93% would provide that information to an EV certificate site.
- Users develop expectations for the green bar. 77% of interviews said if a site they had done business with had stopped displaying the green bar, they would investigate further or abandon a purchase.

 For more information about the Tec-Ed, Inc. study of consumer attitudes about EV SSL certificates, see the study report at <https://www.thawte.com/ucgi/gothawte.cgi?a=o13720307822999007>.

Greater consumer confidence and trust immediately benefit businesses.

Benefits to Businesses

Businesses that use EV SSL certificates can see benefits in terms of brand protection and return on investment (ROI).

Brand Protection

Corporations with established brands face a number of threats online:

- Look-a-like sites that divert traffic from the business' Web site, diluting the incoming traffic and exposing customers to third-party content that appears to be from the legitimate business.
- Spam messages that include the name of a legitimate business and lead users to bogus sites can further dilute traffic to the legitimate site and damage the victim's trust in the brand.
- The continued threat of phishing. MillerSmiles, an anti-phishing service, reported in early 2007 that the average cost to a phishing victim was \$850—five times the previous year's cost (Source: MillerSmiles, "Phishing Trend Continues" available at <http://news.millersmiles.co.uk/article/0064>).

The overall impact of these kinds of threats is that customer identities are stolen and legitimate brands are associated with fraud.

The combined threats of brand jacking from look-a-like sites and phishing can be addressed with the use of EV SSL certificates. Customers will have confidence that they know who they are dealing with and the business is in fact a legitimate enterprise. This in turn can help stem the erosion of trust that can occur if a business name or even industry is commonly associated with phishing scam.

Reduced transaction abandonment and increased customer trust

The financial benefits of EV SSL certificates can be easy to quantify by simply looking at customer behavior. Consider, for example, the case of DebtHelp.com, a financial services firm offering debt management assistance. The financial services industry witnessed a decline in trust of online services stemming from widespread concerns about phishing and other forms of online fraud. The company deployed EV certificates to provide potential customers with a high level of assurance that they were dealing with a legitimate business and that they could disclose personal and financial information without fear of becoming a victim of a phishing scam.

The benefits of deploying EV certificates and establishing greater trust with customers included:

- An 11% increase of transaction completion by Microsoft Internet Explorer users
- An projected 5% increase in revenues over a 2-year period
- A 16,000% ROI
- A decrease number of inbound calls to the company service center resulting in overhead savings
- Perception on the part of customers that businesses that employ EV SSL certificates are taking extra measures to protect their data and identities.

As this case demonstrates, the use of EV SSL certificates can improve conversion rates of visitors and, presumably because there is greater trust in the Web site, reduce the demand for higher-cost telephone support services.

 Full details about the DebtHelp.com case study can be found at <http://www.verisign.com/static/042693.pdf>.

The use of EV SSL certificates creates a win-win situation for both businesses and for browser users. Users can feel confident that they are doing business with legitimate enterprises while expanding their range of choices beyond businesses that are physically accessible. Businesses can expand their base of customers, improve conversion rates and demonstrate higher levels of customer care.

Summary

The SSL protocol continues to be an essential element of securing Internet communications and transactions. With the advent of phishing and online fraud, it became clear that conventional SSL certificates and browser features were insufficient to preserve trust between online business operations and their customers. The problems stemmed from:

- The average user's limited understanding of security measures such as authentication and encryption
- The increasing prevalence of phishing
- The inability of users to access or understand certificate details that would help identify fraudulent sites
- The ability of scammers to acquire SSL certificates and offer some semblance of legitimacy to casual observers

EV certificates addressed these problems with changes on the part of both CAs and browser vendors. CAs offer a standardized and more comprehensive identification and authentication process and new high security browsers have added prominent visual cues to give users a mechanism to quickly identify highly authenticated and therefore safe websites. Studies have shown this combination has succeeded in improving customer confidence and trust that in turn results in increased revenue from online sources.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.