VeriSign®

DATA SHEET

How Extended Validation SSL can help to increase online transactions and improve customer confidence

+ The Problem of Phishing and Online Fraud

Phishing scams and online fraud have created an environment of fear and doubt among online shoppers. New phishing sites are emerging at an alarming rate (the number of unique phishing web sites detected by the APWG rose to 25,328 in December 2007, an increase of more than 7% since the month of November)[1]. Phishing is a problem that affects all of us. Even if you are not a target, phishing casts its net far and wide and it has a detrimental effect on consumer confidence:

- 78% of the UK population worry about identity theft[2]
- 43% have experienced identity fraud or know someone who has[2]
- 84% believe businesses are not doing enough to protect them[2]

To regain consumer trust, site owners need an easy, reliable way to show customers that their transactions are secure and that the Web site is legitimate. To help face up to such threats, security vendors and Internet browsers have combined forces, under the CA Browser Forum, to establish the Extended Validation Standard for SSL Certificates.

+ The Solution

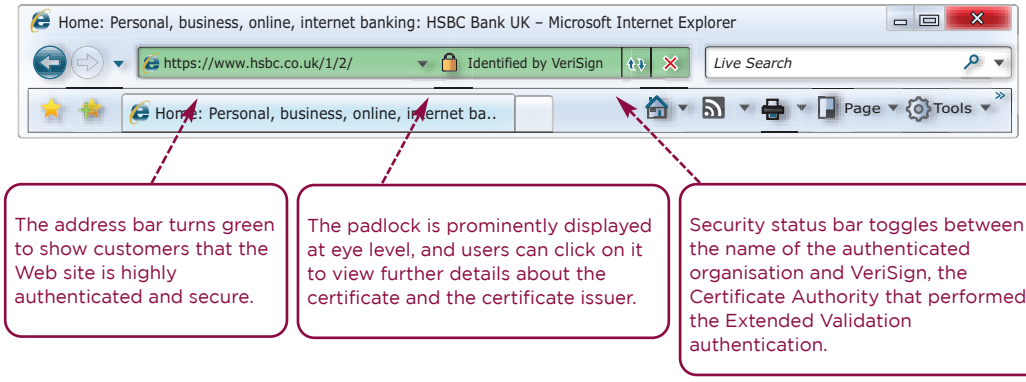
Safely navigating the Internet has become increasingly difficult and the leading browsers have responded to this with increased security measures. The latest browsers including Microsoft Internet Explorer 7 (IE7), Firefox 3.0 and Opera 9.5 can now detect the presence of Extended Validation (EV) SSL Certificates and display unique interfaces to identify the presence of such certificates. The introduction of new color schemes and security status bars in these new browsers, when detecting an Extended Validation SSL Certificate, now help users to make better and safer decisions when transacting online (shopping, banking etc).

+ The Green Address Bar of Extended Validation SSL

Now when shoppers visit a Web site secured with an Extended Validation SSL Certificate, the latest browsers trigger the address bar to turn green and display the name of the organisation listed in the certificate as well as the certificate's security vendor (the vendor is shown only in IE7).

1. Anti-PhishingWorking Group, December 2007
2. YouGov Research, March 2008

A secure connection has been established between browser and Web site, and the Web site has been authenticated according to rigorous industry standards. In the example below the browser controls the display, pulling information from the SSL Certificate and displaying it in the address and security status bar. making it extremely difficult for phishers and counterfeiters to hijack your brand and your customers.

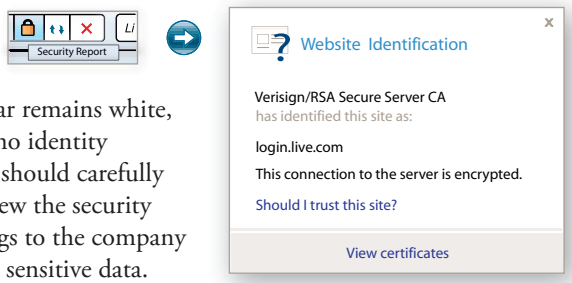


Microsoft® Internet Explorer 7, Firefox 3.0[3] , Opera 9.5 and future versions of these browsers will all support Extended Validation SSL and trigger the green bar. As of July 2008, these browsers accounted for over 70% of the systems in use in the UK, with Internet Explorer 7 covering 53.85% of the market[4].

+ Alternatives to the Green Bar in Internet Explorer 7

The White Address Bar

When you are about to enter sensitive information (e.g. personally identifiable information, usernames and passwords, bank accounts, etc.) you should always look for the secure session - https:// and the Security Status Bar and proceed according to the colour coding of the Address Bar (white, green and red).

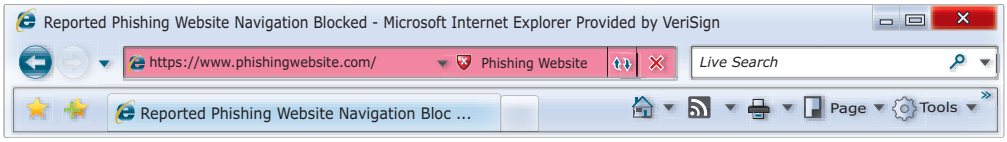


If a secure session starts (https) and the bar remains white, then the page is encrypted with SSL but no identity information is available. In this case, you should carefully read the full URL in the address bar or view the security report, and verify that thisWeb site belongs to the company you intended to visit, before entering any sensitive data.

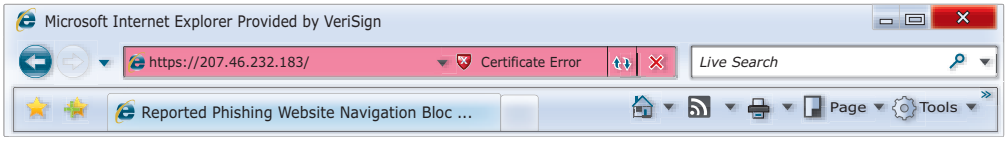
3. The release of Firefox 3 has facilitated Extended Validation SSL. Release notes - http://www.mozilla.com/en-US/firefox/3.0rc1/releasenotes/#whatsnew
4. UK Browser Version Market Share July 2008 – source: http://marketshare.hitslink.com/ Internet Explorer 7 - 53.85%, Firefox 2.0 - 13.57%, Firefox 3.0 - 2.39%, Opera 9.x - 0.54%.

The Red Address Bar

The use of the colour red is a warning to all visitors. Either the site visited is a known phishing site that is misrepresenting its identity…



...or a problem exists with the SSL Certificate used (e.g. it has been revoked or the certificate has expired).



In both cases, make sure that you have typed the correct Web address. If the error persists, you shouldn't browse further or enter any data into this Web site.

+ Alternatives to Green Bar in Firefox 3.0 and Opera 9.5

The Mozilla Firefox browser reflects security indicators to the left of the address bar. If the button to the left is white, the site does not use encrypted communication and therefore the user is not recommended to reveal any potentially sensitive data. If the button to the left of the address bar is blue, the site has recognised certification. If the user clicks on the button, the type of certificate and the name of the issuing CA appear. If the button is green, then the site has the maximum level of certification: an Extended Validation SSL certificate. If the site has any certification problem, the browser will not open it and a warning message will appear to the user.

Opera shows security information to the right of the address bar. White means that the site communication is not encrypted. Yellow indicates that the website has some level of certification. The colour green is again used to denote that the website has an Extended Validation SSL certificate.

+ The Perception of the Green Bar

In January 2007, Tec-Ed[5] researched usage and attitudes of 384 online shoppers and measured their responses to Web sites with and without green bars:

- 100% of participants notice whether or not a site shows the green EV bar
- 93% of participants prefer to shop on sites that show the green bar
- 97% are likely to share their credit card information on sites with the green EV bar, as opposed to only 63% with non-EV sites
- 77% of participants report that they would hesitate to shop at a site that previously showed the green EV bar and no longer does so
- 88% trust the name VeriSign on a site, as opposed to only 22% for the next most trusted SSL provider

5. Tech-Ed Consumer Research – January 2007 - http://www.verisign.com/static/040655.pdf

DATA SHEET

+ The Value of Extended Validation SSL

By making your Web site security more instinctively obvious you too could see the same results that others have[6]:

Scandinavian Design OnLine - 8% increase in conversion rates[6]
"The best part of EV SSL for us is the fact that in the first two months of implementation we saw an 8% positive increase in our online conversion rates. With well over 50% of our customers seeing the green bar today we have high hopes for the future impact that the green bar and EV SSL will have on our conversion rates".
Jörgen Bödmar, CEO, Scandinavian Design OnLine AB

Overstock.com - 8.6% reduction in abandonment rates[6]
"As a result of the enhancement, site visitors with browsers which interface with the new EV SSL Certificates now abandon their shopping cart 8.6% less than visitors without an EV-enabled browser".
Geoff Atkinson, Marketing Chief of Staff, Overstock.com

Opodo - 10% increase in completed sales[6]
"We posted the VeriSign Secured Seal on the payment pages and found that completed sales rose by approximately 10% in comparison to the previous week's results. We immediately realised the impact that the trust factor can have on shopping basket abandonment rates".
Warren Jonas, Head of Service Management, Opodo

Visit us at www.VeriSign.co.uk for more information.

6. Your company's results may vary. VeriSign makes no warranties of any kind (whether express, implied or statutory) with respect to the services described or the information contained herein.

Decypher Media 25/9/2008
00024686