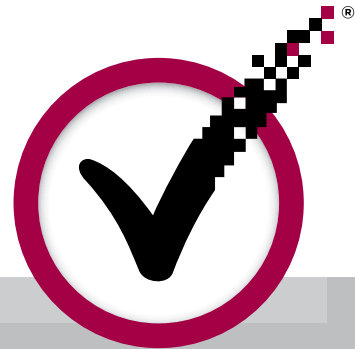




REPORT



HOW TO WIN CUSTOMERS AND BUILD TRUST ONLINE

WHAT SMART COMPANIES ARE DOING
TO BUILD TRUST AND USE IT TO CREATE
COMPETITIVE ADVANTAGE ONLINE



➤ HOW TO WIN CUSTOMERS AND BUILD TRUST ONLINE

What smart companies are doing to build trust and use it to create competitive advantage online.

Businesses with websites need customers' trust. It costs a lot of money to build a good website. Even more to build a brand and advertise it. It's an expensive failure if you lose customers at the final hurdle simply because they don't feel confident enough to buy. Worse; it's bad business. It's like running a marathon and then stopping just before the finish line.

PERCEPTIONS OF RISK

Internet problems receive a lot of attention in the media and consumers are nervous. For businesses, this means some people don't transact online at all. Some are very picky about who they deal with, rejecting sites that don't reassure them. Others will go all the way through to checkout but then abandon the transaction if they feel that their personal information is not well protected.

Get Safe Online, a UK government site sponsored by VeriSign, reveals a number of statistics about people's willingness to transact online. While many people are happy to shop, bank and buy holidays online, many are not. Around a third of the population avoid transacting online¹. Many people have been victims of a computer virus (34 percent), phishing (22 percent), online scams (15 percent) and identity theft (21 percent).

TRUST IS A COMPETITIVE ADVANTAGE

All the things that e-commerce managers want to do – reduce the number of abandoned carts, increase order values, defend margins, increase return on investment from advertising or compete with big name brands – depend on trust. Moving beyond online retail, trust is even more important. Financial or insurance transactions, for example, require customers to disclose even more information than an online purchase. Public sector applications are even more demanding. Would you do your tax return or access your medical records on a site you didn't trust?

If you can make your site more trustworthy, you can turn these concerns to your advantage. Trust can be a competitive advantage.



34%

of people have been victims of a computer virus.

¹ Get Safe Online Report 2009: http://www.getsafeonline.org/nqcontent.cfm?a_id+1517.



REAL COMPANIES, HARD DATA

We carried out a survey of 168 IT managers in United Kingdom and Ireland to understand what businesses worried about and what they did to win customers and build trust online.

First we asked them what they thought their customers worried about. This is a good indication of the sorts of threats that companies want to try to forestall. (i)

The biggest perceived risk was financial loss or fraud followed closely by identity theft. These results seem to reflect media coverage of online crime and results from surveys of end-users, such as the UK government's Get Safe Online annual report. This suggests that IT managers should pay extra attention to proving that their website appears to be what it says it is, showing that customers are safe to entrust their credit card information to the site and that their data won't be intercepted by criminals.

When we asked what the IT managers themselves worried about, the story was a little different. The experts were less concerned about identity theft or phishing. Instead, the biggest concern was ensuring that customers felt safe. But practical concerns were also strong. For example, the fear of unexpected SSL certificate expiry was a major issue. (ii)

These concerns are also understandable. Site spoofing is a real threat; around 911 brands were hijacked in the last quarter of 2009². Phishing can undermine a brand's reputation by creating fake emails and websites using well-known brands. All this suggests that companies need to pay attention to proving that their site is legitimate and not an imposter or fake site. Fear of identity theft is the main reason for people's lack of confidence online³ so website owners need to show that personal information will be properly protected, for example by encrypting it.

Out of date SSL certificates are a huge threat to confidence because they trigger alarming (and alarmingly technical) error messages in web browsers. It's surprisingly easy to lose track of renewal dates, especially if you have many SSL certificates to

manage. IT managers need to manage them efficiently and ensure that they do not expire accidentally. (iii)

We also asked what steps our respondents took to increase trust and safety. The use of SSL certificates to encrypt confidential information was clearly the most popular measure, but a surprisingly small number of

people used the most secure, most visible form of SSL certificate - Extended Validation (EV) SSL Certificates. Few used trust marks such as the VeriSign Secured[®] Seal and even fewer offered visitors any explanation of how they are protected, for example with a 'security advice' page. It seems that website managers are missing a few tricks.

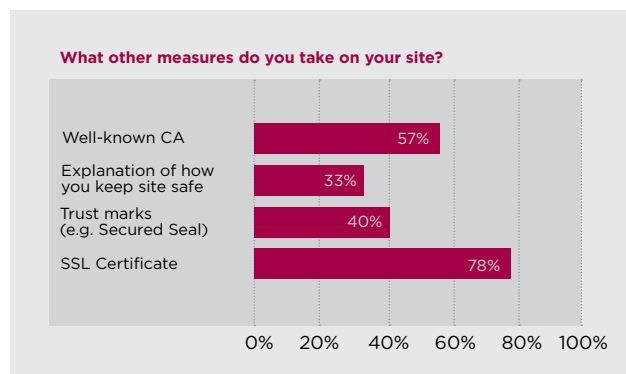
(i)



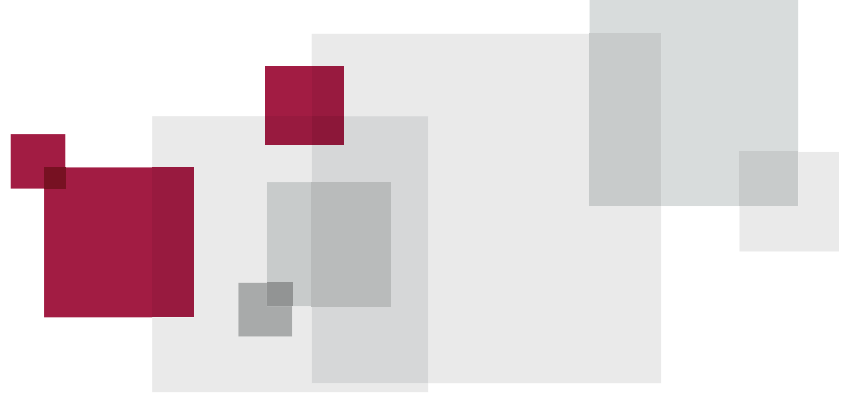
(ii)



(iii)



² Anti-Phishing Working Group, December 2009 www.apwg.org
³ 2009 Synovate/GMI study



❖ BENEFITS OF EXTENDED VALIDATION SSL CERTIFICATES

What does trust and confidence actually mean? In part, it is a reaction to online criminality such as identity theft. In part, it is about changing customer perceptions of safety. We have broken these issues down into four categories:

- Seller authentication ('we are who we say we are')
- Data protection and encryption ('we protect your data')
- Brand enhancement ('we respect your privacy')
- Increased confidence ('you're safe shopping here')

Extended Validation (EV) SSL Certificates upgrade conventional SSL certificates to display the company name and a green background in the address bar on compatible browsers such as Internet Explorer 7 and above, Firefox 3.0 and above and on the latest smartphones. Users get highly visible proof that the website is trustworthy.

They address all four points:

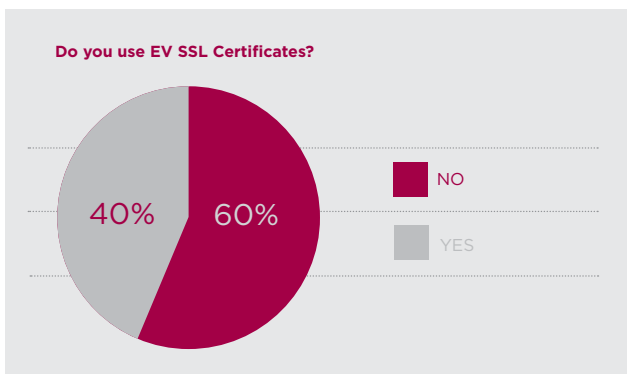
- **Seller authentication.** VeriSign applies strict authentication procedures before issuing a certificate so that site users can be sure that the site is not a fake.
- **Data protection and encryption.** EV SSL Certificates offer the highest level of encryption available with an SSL certificate so that users' data is encrypted between the browser and the site owner.
- **Brand enhancement.** With a compatible browser, EV SSL Certificates display the company name in the browser's address bar so that users can see that the site belongs to the company they think it belongs to.
- **Increased confidence.** The green address bar of a site protected by an EV SSL Certificate is a visible and trusted sign of enhanced security for users.

ABOUT EXTENDED VALIDATION SSL CERTIFICATES

Extended Validation SSL Certificates were created in direct response to the rise in Internet fraud, eroding consumer confidence in online transactions. The Extended Validation SSL Standard raises the bar on verification of SSL Certificates and enables visual displays in high security browsers.

In 2006, a group of leading SSL Certificate Authorities (CAs) and browser vendors approved standard practices for certificate validation and display called the Extended Validation Standard. To issue an SSL Certificate that complies with the standard, a CA must adopt the extended certificate validation practice and pass a Webtrust audit. The validation process requires the CA to authenticate the certificate applicant's domain ownership and organizational identity, as well as the individual approver's employment with the applicant, and authority to obtain the Extended Validation SSL Certificate.

Extended Validation SSL Certificates give high-security Web browsers information to clearly identify a Web site's organizational identity. For example, if you use Microsoft® Internet Explorer 7 to go to a Web site secured with an SSL Certificate that meets the Extended Validation Standard, IE7 will cause the URL address bar to turn green. A display next to the green bar will toggle between the organization name listed in the certificate and the Certificate Authority (VeriSign, for example). Firefox 3 also supports Extended Validation SSL.





REAL-WORLD RESULTS

Our survey revealed that companies that deployed EV SSL Certificates saw increased order values, fewer abandoned carts and increased sales, but the biggest gain was better customer perceptions of site security. An overwhelming majority of respondents (78 percent) reported this result. We see the same results again and again with our customers. Businesses that secure their websites with VeriSign EV SSL report an average increase in transactions of over 20 percent⁴. Recent case studies of VeriSign customers who use EV SSL Certificates show significant benefits*:

- Misco, an electronics retailer, saw a five percent reduction in abandoned carts
- Directline holidays saw conversions increase by eight percent
- QuickRooms.com's sales increased by nearly seven percent
- Papercheck.com nearly doubled online registrations (up by 87 percent)
- CarInsurance.com increased online enrolment by 18 percent
- Fitness Footwear increased conversions by 16.9 percent and had 13.3 percent fewer abandoned carts
- CreditKarma.com boosted conversion rates by 26 percent

VERISIGN RECOMMENDATIONS

There are five simple steps that you can take to increase users' trust and confidence:

- **Upgrade to EV SSL.** SSL is good, Extended Validation SSL is better. They replace conventional SSL certificates, cost little more and require little extra work to deploy.
- **Select a trusted Certificate Authority.** The reputation of a Certificate Authority (like VeriSign) is important to users. In a survey, 88 percent of participants said that they trusted VeriSign, compared with just 22 percent for the next most trusted provider⁵.
- **Use a trust mark.** Back up EV SSL Certificates with extra visual cues that show you value customers' security. It helps if this kind of trust mark is widely recognised. For example, 81 percent of UK online shoppers recognise the VeriSign Secured[®] Seal, significantly more than any other trust mark.⁶
- **Improve certificate management.** Audit your certificates to make sure that you get automatic warning of upcoming expiration dates. Consider consolidating all your certificates into a managed account. The VeriSign Certificate Center will help you manage VeriSign Certificates online in one central location. If you use certificates from multiple Certificate Authorities or you have many certificates, invest in a management tool such as VeriSign Managed PKI for SSL.
- **Explain to users how you protect them.** Adding a page to your help section or footer menu that explains how you protect users, for example by describing what an SSL certificate does, can help to reassure users.

We found that, on average, survey respondents spent 16 percent on security measures. This is a significant proportion of their spending and yet many companies were not taking these basic steps to enhance customer trust, safety and confidence on their sites.

Although they require a modest investment of time, for example to modify a page design to include a trust mark, they are not expensive either in absolute terms or as a proportion of website security budgets.

EV SSL is here to stay. Smart companies are already using it and consumers increasingly understand the benefits and immediately see when a site uses it. However, many companies - including some of your competitors - still do not use it. Nor do they take other steps to build user trust and confidence. As a result, implementing EV SSL and taking all the other recommended steps is a compelling business choice. Winning customers' trust and confidence is a competitive advantage and VeriSign can help you do it.



81%

of UK online shoppers recognise the VeriSign Secured Seal.

⁴ As of December 2009, in tests conducted by dozens of websites around the world, VeriSign EV SSL Certificates helped to provide an increase in conversions ranging from 5 percent to 87 percent and averaging over 20 percent.

⁵ Tec-Ed, Jan 2007

⁶ 2009 Synovate/GMI study

➤ ABOUT VERISIGN

VeriSign (NASDAQ: VRSN) is the trusted provider of Internet infrastructure for the networked world. Billions of times each day, our SSL, identity and authentication, and domain name services allow companies and consumers to engage in trusted communications and commerce. For more than 10 years, VeriSign Internet infrastructure has been at the very heart of the Internet, enabling key transactions and protecting valuable data.

VeriSign is the leading Secure Sockets Layer (SSL) Certificate Authority enabling secure e-commerce and communications for websites, intranets and extranets. VeriSign continues to lead the SSL certificate industry as a member of the CA/Browser Forum, a voluntary organisation currently focused on EV SSL Certificates.



Visit www.Verisign.co.uk for more information.

*Your company's results may vary. Factors specific to these customers may have helped contribute to their results. Contact VeriSign today to talk about how we can best address your company's security needs.

