Symantec. | Website Security Solutions

Norton SECURED powered by Symantec

How trust really affects online shoppers' decision to buy

Symantec Report

How trust really affects online shoppers' decision to buy

'Trust is the linchpin for everything we do in our digital world,' *says Gartner.*[1]

People need to trust the websites they visit and the businesses they interact with; they need to trust that their personal information is secure and that it's being handled correctly.

Above all, people need to trust that organisations are doing all they can to combat cybercriminals and the sophisticated attacks they deploy to undermine and exploit the online economy.

How convinced are online consumers?

Trust is essential, but just how well are website owners doing at building trust with their potential online customers?

Symantec commissioned an online survey in the UK, US, France and Germany from YouGov to understand the level of anxiety and security consciousness among shoppers and to see if signs of security influence people's willingness to buy online.

The results are clear: people are worried about security issues when shopping online, but the majority of people know what to look for to protect themselves.

Organisations are often told to use Extended Validation SSL certificates, monitor SSL expiry closely and deploy trust marks across their websites but do shoppers really respond to these steps?

Our survey says: yes.

People feel more confident completing a transaction on a website they trust and it's these steps that people look for when deciding whether or not to trust a website.

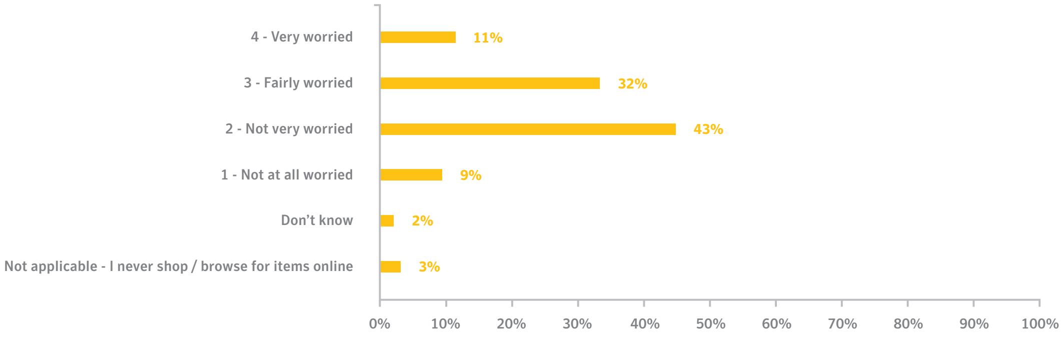
In other words, fail to maintain effective website security and you'll fail to build trust with customers. And without trust, you can kiss your conversions goodbye.

[1] NetworkComputing. Expired Digital Certificates: A Management Challenge - http://www.networkcomputing.com/networking/expired-digital-certificates-a-management-challenge/d/d-id/1102269

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 7,541 adults, with 2,102 from the UK, 1,011 from France, 2,050 from Germany and 2,378 from the US. Fieldwork was undertaken between 3rd - 8th September 2015. The survey was carried out online. The figures have been weighted and are representative of all adults (aged 18+ in each market).

How worried are your customers?

Q1 **Thinking about when you ever shop / browse for items online.. In general, how worried, if at all, are you about the security issues of shopping online (e.g credit card fraud, identity theft, etc) ?**



Base: All adults online (7541)

There's no doubt: when it comes to online shopping, a lot of people are worried about security issues. In our survey, 43 percent of respondents were 'very' or 'fairly' worried and only a meagre nine percent said they were not worried at all.

Websites owners have to accept that trust and security are important to consumers. Obviously factors like price, product quality and user experience matter too, but security cannot be ignored.

In particular, a fifth of people who ever shop/browse online are most worried about stolen payment details. Nearly as many (19 percent) are most worried about identity theft and in the US this figure spikes to over a third (36 percent). These concerns speak very specifically to the security of the data that customers hand over and the credibility of the people or companies they hand it over to.

This underpins the critical importance of credible (there's that word again) SSL/TLS certificates, issued by recognised and trusted Certificate Authorities, such as Symantec. They encrypt personal and payment data and they verify the identity of a website owner, and thereby address people's two biggest concerns.

Why are people worried?

It's no wonder people are worried: 32 data records[2] were lost or stolen every second in 2014 and 80 percent[3] of identity theft in the first three months of 2015 was attempted or perpetrated online.

[2] Nasdaq. Credit card fraud and ID theft statistics - http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388#ixzz3mZTIPqsa

[3] BBC News. Number of identity theft victims 'rises by a third' - http://www.bbc.co.uk/news/uk-32890979

And why are these numbers so high? Because people's data is valuable to criminals. Symantec's most recent Internet Security Threat Report[4] reported that credit card details sell online for anything between $0.50 and $20 on the black market and, depending on its completeness, identity information can fetch between $10 and $50.

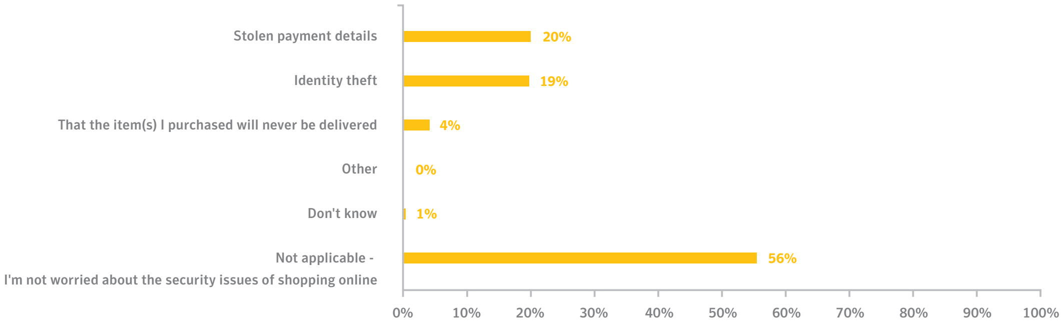
Of course it's not just the data breaches and cases of card fraud themselves that are making people wary of online transactions; it's the increasing amount of media coverage that cybercrime and sensational hacks are now receiving in the press.

The recent Ashley Madison attack is a perfect example, with reports of suicides and celebrity scandals adding lurid details to the already-intriguing story of the attack on the extra-marital dating website.

Add to that government breaches like the Office of Personnel Management attack earlier this year[5], which affected the personal data of nearly four million US government employees, and fear is inevitably going to rise. If people can't trust their own government's cyber security, then they are hardly going to extend their trust to an ecommerce website without some serious persuasion.

A lack of concern doesn't mean a lack of awareness

Q2 You said you are worried about the security issues of shopping online... Which one, if any of the following are you most worried about when shopping online? (Please select the option that best applies)



Base: All adults online who ever shop/browse for items online (7330)

Of course, while some people have very specific concerns about online shopping, our data also shows that 56 percent of our respondents are not worried about the security issues of online shopping at all. It's important to realise, however, that this doesn't mean they don't care about security.

As you will see later in this report, a surprisingly high percentage of people look for signs of credibility and trust such as 'https' and a padlock in their web browser address bar. It is likely that this significant number of respondents, who say they are not worried, say so because they understand the risks and they know how to avoid them.

[4] Symantec. 2015 Internet Security Threat Report, Volume 20 - http://www.symantec.com/security_response/publications/threatreport.jsp

[5] BBC News. Millions of US government workers hit by data breach - http://www.bbc.co.uk/news/world-us-canada-33017310

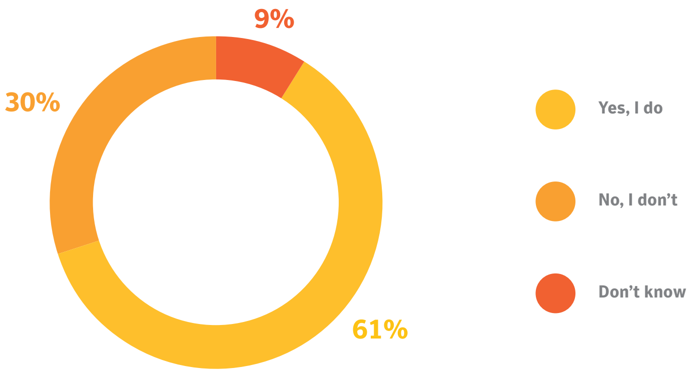
The importance of a reputable address

In the physical world, where you're located can make all the difference to your credibility. Think of tailors on Savile Row in London, designers on 5th Avenue in New York or pretty much any store on the Champs-Élysées in Paris. When you walk into a retailer in any of those locations you know what you're going to get.

The same applies online: how your URL address appears can make a big difference to how you are perceived by your customers.

We asked our survey respondents if, in general, they tend to pay attention to the browser address bar when purchasing an item online. The results might surprise you:

Base: All adults online who ever shop/browse for items online (7330)



Almost two thirds of online shoppers look at the URL address bar when purchasing online to tell them if the site they are on is secure, but what are they looking for?

The main indicators of trust are:

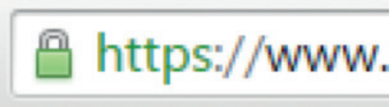
- **The 'https'** (as opposed to an unencrypted 'http') at the beginning of the address that tells them their interaction with the website is encrypted, so criminals can't eavesdrop on the information they send to make a purchase.

- **A grey padlock,** which tells them that the people who run the site have bought the domain – but it doesn't confirm who that owner is.

- **A green padlock,** which indicates the site has Extended Validation SSL, which means the site owner has been through a rigorous identity check to confirm they are who they say they are and they own and control this site.

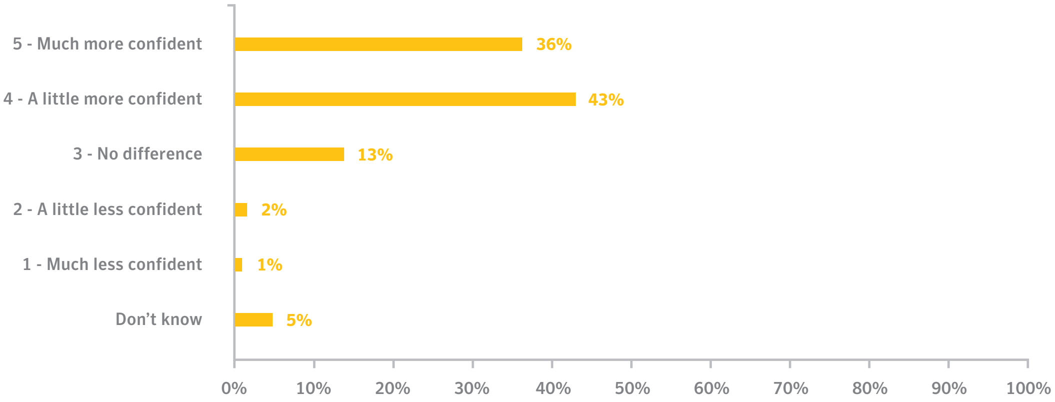
So we know customers are looking, but how are they reacting?

We showed our respondents the following example of a URL address bar with a padlock:



We then asked them how much more or less confident they would be to make an online purchase if there was a padlock in the URL address bar compared to an address bar without a padlock, or would it make no difference?

A staggering 78% when rounding to two decimal places said it would make them feel more confident.



Base: All adults online who ever shop/browse for items online (7330)

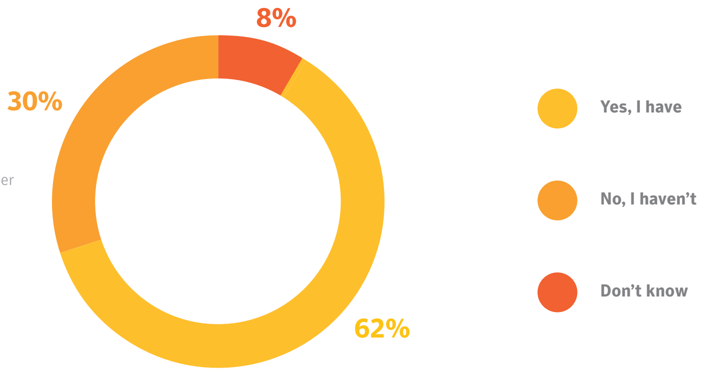
Note that the example we showed them was a green padlock, indicating the site has SSL, which gives them confidence not just in your site, but in your business as well.

So the lesson is clear: when it comes to building trust and credibility, SSL certificates are an essential requirement.

The conversion question: the influence of age

‘Building trust at the onset is the foundation for sustaining lifetime loyalty among shoppers,’ says Nielsen.[6]

Certainly our survey suggests that trust is key to conversion for every demographic. When we asked if our respondents have ever not completed a purchase because they did not trust the website, the response was virtually the same across all ages (and regions for that matter).



Base: All adults online who ever shop/browse for items online (7330)

Failure to build trust with a customer of any age is likely to lead to a lost conversion. But how you go about building that trust needs to be tailored to what different demographics respond to.

The young ones

‘Millennials comprise more than half of respondents (53 percent) who plan to make an online purchase across every product category in the study,’ says Nielsen’s recent report, Ecommerce: evolution or revolution.[6]

Not only are Millennials the bulk of online buyers, but when looking at purchasing behaviour in each category, Nielsen’s research also suggests that, ‘once an online shopper, always an online shopper.’

Earning trust with consumers early on could prove lucrative for years to come, so it’s vital you know how to appeal to younger shoppers.

6. Nielsen. E-Commerce: Evolution or revolution in the fast-moving consumer goods world? August 2014 - http://ir.nielsen.com/files/doc_financials/Nielsen-Global-E-commerce-Report-August-2014.pdf

We showed our respondents two images:

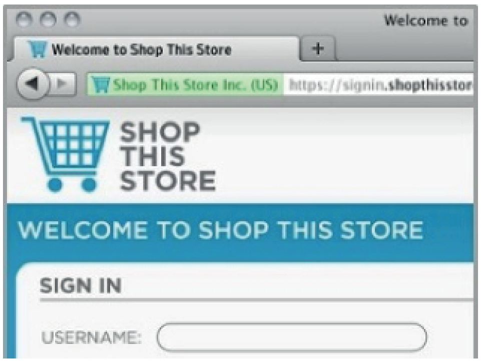

Welcome to
Welcome to Shop This Store
+
Shop This Store Inc. (US)
https://signin.shopthisstor
SHOP
THIS
STORE
WELCOME TO SHOP THIS STORE
SIGN IN
USERNAME:

Image 1

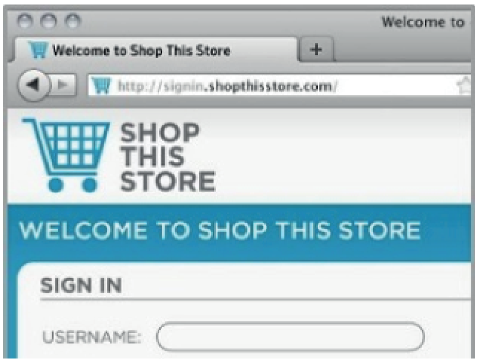

Welcome to
Welcome to Shop This Store
+
http://signin.shopthisstore.com/
SHOP
THIS
STORE
WELCOME TO SHOP THIS STORE
SIGN IN
USERNAME:

Image 2

- **Image 1** shows what a trustworthy website, with Extended Validation SSL would appear as – note the green address bar and the 'https'

- **Image 2** shows no signs of security

Extended Validation SSL is important and recognising it means having a certain level of technical understanding. Well over two thirds (70 percent) of respondents aged 18-to-24 chose Image 1 as the one they would trust more to make a purchase from.

The younger generation are savvier about Internet security. They know what to look for and what to trust when it comes to online shopping, so the most important thing you need to remember when trying to convert young people is exposure.

You need to make it clear you have taken every step you can to prove your credibility and keep their data safe. This means:

- **Extended Validation SSL**, which turns their address bar green

- **Trust marks**, such as the Norton Secured Seal, prominently displayed on your website to show who you're trusted by

- **Always-On SSL** so that every interaction with your site is encrypted, whether your customer is browsing or buying

The not-so-young ones

Euromonitor forecasts[7] that the global spending power of those aged 60 and above will reach $15 trillion by 2020. Not only that, but the stereotype of grandparents struggling to switch on a computer is now completely out of date.

'A disproportionate share of middle-aged consumers are shopping online,' according to Business Insider Intelligence and one in four mobile shoppers in the US is over 55. 'As the population ages, greater percentages of consumers will be connected and online prominence will continue to grow,' echoes John Burbank, President of Strategic Initiatives, Nielsen.

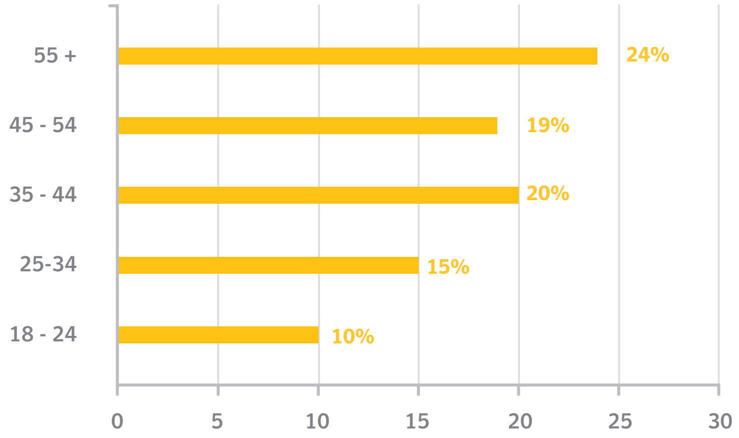
The older generation is a fast-growing, well-off and increasingly tech-savvy population but they need more reassurance than younger shoppers and they need a less technical indicator of that reassurance.

A concerned cohort of shoppers

Going back to our survey, almost half (48 percent) of all respondents aged 55+ said they were worried about the security issues of online shopping, compared to just 34 percent of 18-to-24 year olds.

Similarly, when it came to what, specifically, respondents were most worried about when shopping online, the older the respondent was, on average, the more concerned they were about identity theft.

Percentage of respondents who ever shop/ browse for items online selected 'identity theft' as the option they were most worried about when shopping online



Base: All adults online who ever shop/browse for items online (7330)

At the same time, older shoppers are less technically savvy. When shown the same two website images as the 18-to-24 year olds (one with Extended Validation SSL and the other with no sign of security) only 29 percent of shoppers those aged 55 and above selected the image depicting Extended Validation SSL as the site they would trust more to make a purchase from.

[7] Financial Times. The Silver Economy: Baby boomers power new age of spending. 7 Nov 2014 - http://www.ft.com/cms/s/0/e9fc95c0-44b1-11e4-ab0c-00144feabdc0.html#axzz3mZB73kbn

For this cohort of shoppers you need a simpler way of demonstrating your credibility and our survey suggests trust marks are the ideal answer.

We asked our respondents the following question:
For the following question, please imagine you were shopping online and about to make a purchase…Based on the images below, which ONE, if either, of the following websites would you trust more to make a purchase from?

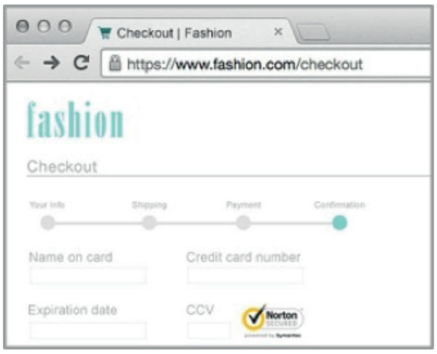


Image 1

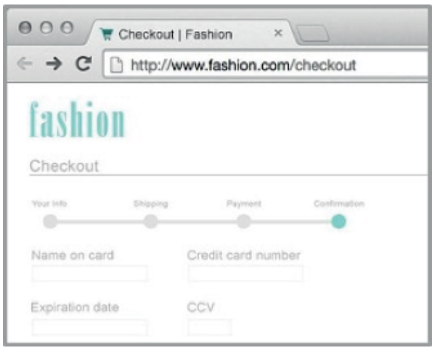
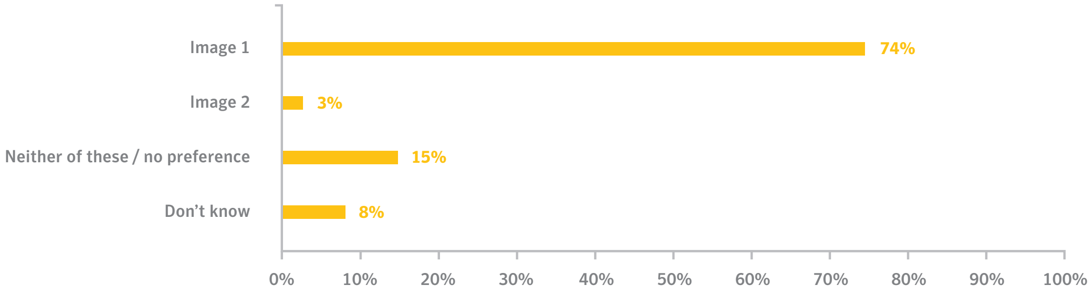


Image 2

Almost three quarters (74 percent) chose Image 1, the image that includes the Norton Secured Seal and this overwhelming preference was consistent across every age group.



Base: All adults online who ever shop/browse for items online (7330)

To appeal across the board, therefore, you need both Extended Validation SSL and the trust mark to reinforce it.

8. Conversion Voodoo. Proper placement of you 'trust logos' will improve conversion rates - http://www.conversionvoodoo.com/blog/2012/05/proper-placement-of-your-trust-logos-will-improve-your-conversion-rate/

What a difference a trust mark makes

As we've seen, no matter your target market, the addition of the Norton Secured Seal can significantly increase how much a customer is likely to trust your website when making a purchase.

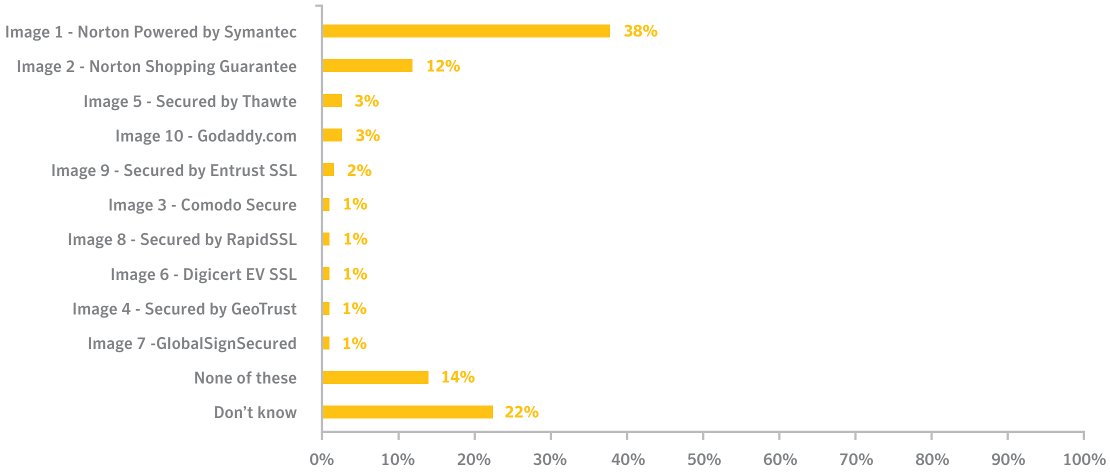
Such trust marks can be placed anywhere you choose on your site, although research has shown that they have the biggest impact next to the most critical or sensitive fields in a form. During one particular experiment[8], switching the position of the trust mark from the top of the page to alongside the form led to a six percent gain in the form's conversion rate.

What's in a name?

It's not just the positioning of a trust mark that affects the impact it can have on a potential customer; the name on the trust mark matters too.

A trust mark effectively says to a website visitor that an independent third party has checked out this website and trusts it, so you can too. It follows, therefore, that a well-recognised, well-trusted third party's opinion will mean more to a potential customer than a name they've never heard of.

We asked our respondents which one, if any, of the following trust marks would they trust the most when making a purchase online. The trust marks were presented in no particular order.



Base: All adults online who ever shop/browse for items online (7330)

The credibility of Symantec speaks for itself: Nearly half (49%) of the respondents selected one of the two Symantec trust marks included in the list: 'Norton Secured Seal' and the 'Norton Shopping guarantee'.

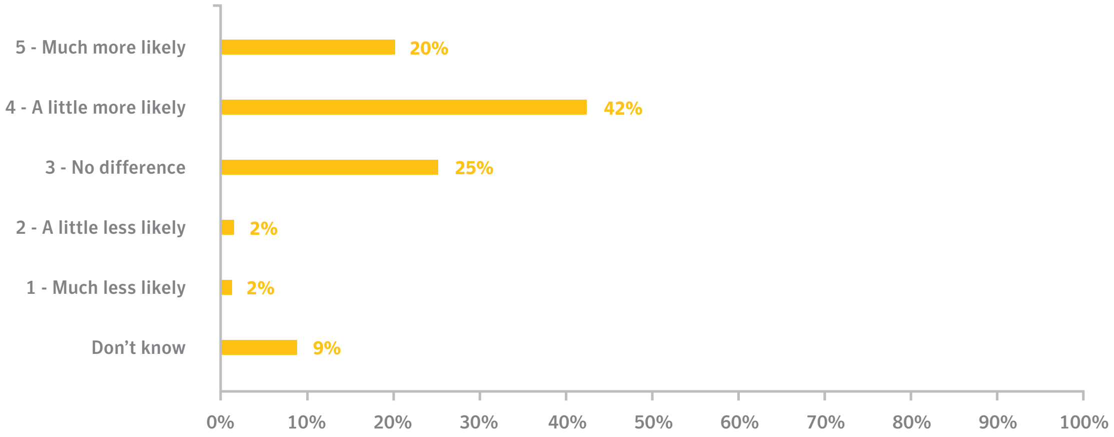
As we've shown in this report, trust is an incredibly important factor for conversion rates, but of course, trust doesn't automatically equate to a purchase. We decided, therefore, to try to understand a little more about the correlation between a Symantec trust mark and a completed transaction.

We showed our respondents the Norton Secured Seal, which is displayed over half a billion times per day on websites in 170 countries.

Norton
SECURED
TM
powered by Symantec

And we asked them, 'how much more or less likely would you be to complete an online transaction/ purchase if you saw this symbol on the payment page of a website?

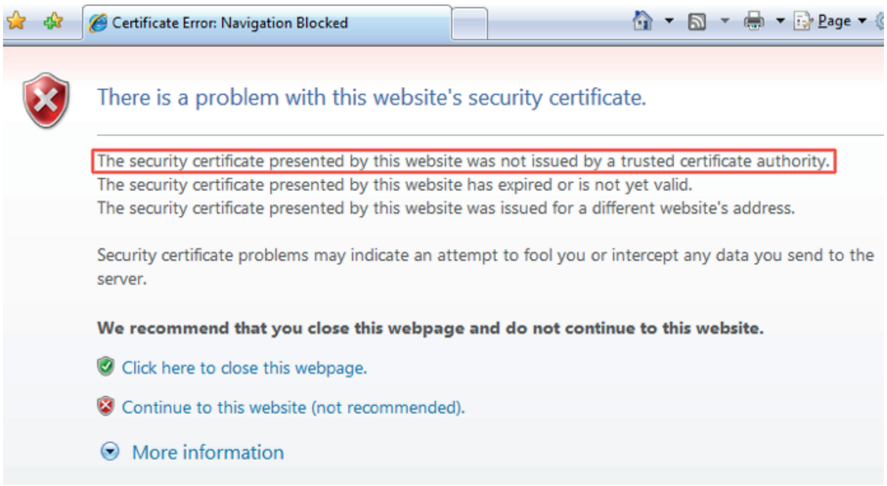
Almost two thirds (63% when rounding to two decimal places) answered more likely.



Base: All adults online who ever shop/browse for items online (7330)

What happens when you fail? How consumers react to security warnings

Building up trust with online consumers is important, but you also need to work hard to maintain it. Fail to update an expired SSL certificate and your site visitors will encounter a security warning similar to the one we showed our survey respondents:



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website has expired or is not yet valid.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

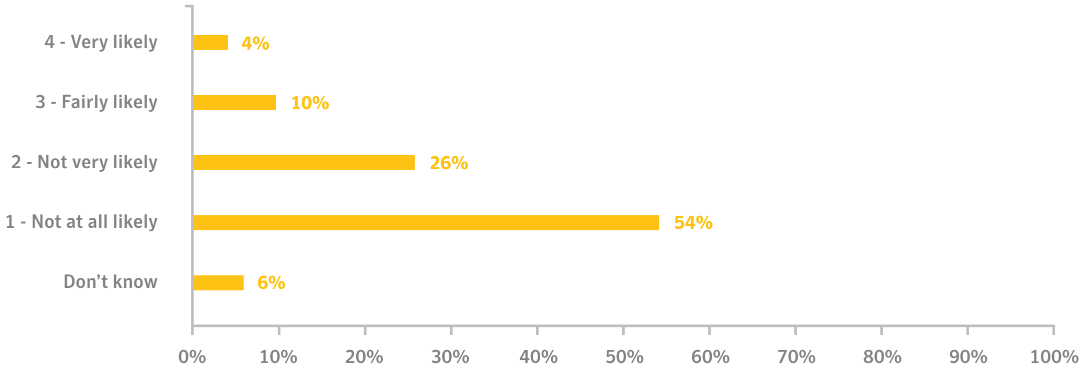
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

We asked our respondents how likely, if at all, they would be to continue to a website they wanted to go to if they saw that warning. The results indicate that most online shoppers see such a warning as a breach of trust, with 80 percent not at all likely or not very likely to continue to their intended site.



Base: All adults online who ever shop/browse for items online (7330)

As with the other results in our survey, the older the respondent, the more likely they were to be put off by such a warning with two thirds of online shoppers 55 and over not at all likely to continue to the website, while only 41 percent of those aged 18-to-24 said the same.

The adverse effects on a website's credibility of security warnings shouldn't come as a surprise. Not only is that exactly what such warnings are designed for – to warn visitors that they cannot necessarily trust the site they are about to visit – but a study conducted[9] by the University of California, Berkeley, confirmed that more often than not, people do pay attention to such warnings:

During our field study, users continued through a tenth of Mozilla Firefox's malware and phishing warnings, a quarter of Google Chrome's malware and phishing warnings, and a third of Mozilla Firefox's SSL warnings. This demonstrates that security warnings can be effective in practice.

As a website owner or security manager, you must therefore refine your SSL management processes and ensure you have complete oversight of your organisation's SSL estate. Advance warning of any expiry dates can be the difference between a customer gained and several potential customers lost.

As the quote from UC Berkeley's study also shows, you need to continually scan your site for vulnerabilities and malware, as malware warnings are also very effective in deterring potential customers from your site. Increasingly, too, search engines scan sites for malware and block infected sites. This can have a catastrophic impact on organic traffic.

[9] Usernix. Alice in Warningland: A large scale field study of browser security warning effectiveness https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe

Location, location, location

Although the majority of this report looks at a set of merged results that YouGov gathered from respondents across the UK, Germany, France and the US, there are a few regional variations within Europe that are worth noting.

The UK: an island of security-savvy consumers

"Good cyber security underpins the entire digital economy – we need it to keep our businesses, citizens and public services safe…Trust and confidence in UK online security is crucial for consumers, businesses and investors."

These are the words of UK minister for the digital economy[10], Ed Vaizey. There is clearly a strong focus on consumer safety and education in the UK and this is reflected in our survey results.

When asked how worried, if at all, you are about the security issues of online shopping, the UK had the lowest number of respondents choosing 'very worried', at just four percent. In fact, almost two thirds, 63 percent, said they were either 'not very worried' or 'not at all worried' – significantly more than the combined figure of 52 percent.

This is likely because UK consumers are better educated about what to look for to ensure they are interacting with a secure website thanks to public campaigns such as Get Safe Online. The UK had the lowest percentage of respondents who shop online said they would be very likely to continue to a website if they saw a security warning, or 11% for very/ fairly likely.

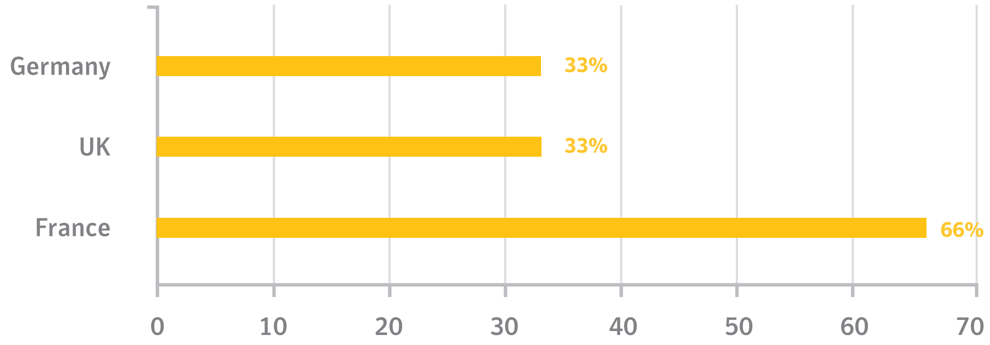
And when shown a URL address bar with a padlock, 43 percent answered that it would make them 'much more confident' to complete an online purchase, much higher than the combined figure of the global average of 36 percent.

[10] ComputerWeekly.com. Majority of UK business have been targeted by cyber criminals.
http://www.computerweekly.com/news/4500253942/Majority-of-UK-businesses-have-been-targeted-by-cyber-criminals

France: a land of nervous shoppers

The French respondents in our survey were significantly more worried about the security issues of online shopping than any other nation, with two thirds of respondents 'fairly' or 'very' worried, compared to the combined figure of just 43 per cent.

Percentage of respondents who answered that they are 'very' or 'fairly' worried about the security issue of online shoppers



Base: All adults online who ever shop/browse for items online (7330)

Half of French respondents who shop online were most worried about stolen payment details; the combined figure was a fifth.

Despite their concerns, however, the French respondents were actually more likely to continue to a website that they wanted go to, despite seeing a security warning. Over a quarter (26 percent) said they were 'very' or 'fairly' likely to continue, whereas the the combined figure was only 14 percent.

If the French are visiting sites with expired or revoked SSL certificates then, of course, they have every reason to be worried.

Germany: a tough crowd to convince

Our survey results suggest that German consumers aren't so reassured by indicators of trust.

When shown a URL address bar with a green padlock, for example, only a quarter of German respondents who shop online said that it would make them 'much more confident' to complete an online purchase. This is in contrast to both the UK and France, where 43 percent of respondents gave the same answer.

Similarly, when shown two images, one of a site with 'https', a padlock and a Norton Secured Seal and a second image with no trust indicators, only two thirds of German respondents chose the first image as the one that they trusted more to make a purchase from, with 21 percent saying they preferred neither. The combined figure, respectively, were 74 percent and 15 percent.

A study published by the German Institute for Trust and Security on the Internet[12] has confirmed that the German public's confidence in the Internet has significantly deteriorated. This could explain why certain indicators of security weren't received so well in our survey.

On the other hand, the State of IT Security in Germany 2014[13], published by the German Federal Office for Information Security reports that:

"Despite increased awareness [of security issues] and loss of confidence [in the Internet], there has only been a very slight increase in numbers taking practical steps to improve their security."

So it may of course be that German consumers haven't taken the time to educate themselves on what to look for when shopping online to ensure their safety.

German website owners clearly face a serious challenge building trust with potential customers. A recent change in the law[14], which states that German website owners can be fined for not staying up to date with the latest in website security, may help to alleviate this problem, but either way, the pressure is certainly on to ensure credibility and security.

12. DIVSI. PRISM und die Folgen: Sicherheitsgefühl im Internet verschlechtert, 3. Juli 2013 - https://www.divsi.de/prism-und-die-folgen-sicherheitsgefuehl-im-internet-verschlechtert/

13. Federal Office for Informattion Security. The State of IT Security in Germany 2014 - https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile

14. Friedrich Graf von Westphalen & Partner. German Bundestag passes IT Security Act - http://www.fgvw.de/2704-1-German+Bundestag+passes+IT+Security+Act.html

How Symantec helps you build trust with customers

Symantec is a leading expert in website security; we secure more than one million web servers worldwide and Symantec SSL secures 91 percent of Fortune 500 companies.

We offer a range of products and services to help you establish and maintain trust with your customers and improve your chances of conversion.

The product	What it is	How it helps build trust
Symantec SSL/TLS certificates	We offer a range of SSL certificates to help you secure both external and internal websites.	SSL certificates confirm who the owner of a website is and ensure any data exchanged between the visitor and your website server is encrypted, so criminals can't eavesdrop.
Extended Validation SSL	We undertake a rigorous business identity check to ensure you are who you say you are and that your business is registered with the relevant governing bodies.	Extended Validation SSL turns a visitor's address bar green and/or displays a green padlock. It tells your customer that you are who you say you are and that you're a reputable organisation.
Norton Secured Seal	As shown in the report, you can use this trust mark on your website when you secure your site with Symantec SSL.	It tells visitors that a well-known third party trusts your site. Our survey shows that customers respond well when they see it on a site and previous studies have shown it is the most recognised trust mark on the Internet.
Seal-in-Search	For customers who use browsers enabled with security plug-ins, this displays the Norton Secured Seal next to your website on search engine results, partner shopping sites and product review pages.	This helps to establish trust with a customer before they've even visited your site, encouraging them to click and choose you over your search engine competitors.

The product	What it is	How it helps build trust
Norton Shopping Guarantee	This provides three, 30-day guarantees to your customers: • ID Theft Protection up to $10,000. • A full 3rd party guarantee of your purchase terms of sale of up to $1,000 • Lowest Price Guarantee up to $100.	This reassures the customer that you have faith in your own site and that they won't lose out, should the worst happen.
Vulnerability and malware scans	Included with certain Symantec SSL certificates you receive free, automatic weekly vulnerability and daily malware scans.	In 2014, three quarters of scanned websites[4] were found to have vulnerabilities, a fifth of which were critical. Leaving yourself exposed to malware puts your customers at risk and increases the chance of your site triggering a security warning. Regular scans help you avoid this.
Discovery and Automation	Symantec's Discovery and Automation tools help you manage your SSL estate, ensuring you have no rogue certificates and that an approved Certificate Authority has issued all certificates. You also receive advance warning of any upcoming SSL expiry dates.	As we've seen, expired SSL certificates dismantle the trust you've built with customers. As a company grows, it gets hard to keep track of multiple SSL certificates, increasing the risk of a missed renewal. Symantec's tools help you avoid this situation.

To find out more about building trust with a world-renowned cyber security partner, get in touch with Symantec today.

[4] Symantec. 2015 Internet Security Threat Report, Volume 20 - http://www.symantec.com/security_response/publications/threatreport.jsp

Symantec. Website Security Solutions

Norton SECURED powered by Symantec

More Information

Visit our website
www.symantec.co.uk/ssl

To speak to a Product Specialist in the UK call:
0800 032 2101 or **+44 (0) 208 6000 740**

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organisations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec UK

Symantec (UK) Limited.
350 Brook Drive,
Green Park, Reading,
Berkshire, RG2 6UH, UK.