Symantec | Website Security Solutions

Norton SECURED powered by Symantec

Simple Steps to a Secure Website in 2016

WEBSITE SECURITY GUIDE

384 million identities were exposed in 2014 as a result of data breaches. That's equivalent to the whole population of Western Europe.

If your website is weak enough to let in a hacker, not only could you face the wrath of angry customers, but you could also be exposed to regulatory fines and damaging media coverage.

Why having a secure website is worth it

Your website has huge potential to help your business grow. It also has huge potential to damage your business. We're not here to scaremonger with big statistics and techno-jargon but understanding the risks is as important as appreciating the opportunities. And that starts with understanding what your customers are doing on your site:

✔ Buy something

As fewer shop in stores, online retail is set to account for 21.5 percent of total retail sales by 2018 from 12.7 percent today, the highest online retail share in the world.

Online shopping is a vital part of the economy, but shoppers are increasingly wary. They want proof that you're doing all you can to protect their data before they part with their card details.

✔ Read your blog

Nearly half of customers read reviews and blogs before purchasing online, according to ecommerce software specialists, Selz. In fact, 13 percent said that a blog post had inspired a purchase.

Increasing visitors to your blog means more than quality content: you need a secure site that doesn't put readers at risk of malicious software and stays in Google's good books.

✔ Fill in their details on a landing page

Inbound marketing costs 61 percent less per lead than traditional techniques. Not only that, but marketers who have implemented inbound marketing strategies achieve almost double the conversion rate of non-inbound marketers, from 6 to 12 percent.

You definitely don't want to put people off sharing their contact details with you on a landing page because they don't trust your site.

✔ Complete another sort of transaction, for example, booking appointments

People have become accustomed to efficient, easy-to-access, 24/7 shopping thanks to sites like Amazon and your visitors now expect that same online convenience for other interactions.

When your website visitors can book an appointment or complete another sort of non-financial transaction online it allows them to interact with you on their own terms and it keeps your doors open for business.

✔ Sign up for a free trial

'Smart companies know giving away freebies is a great way to lure in customers,' argues 37Signals.

Free versions of apps or other software helps potential customers experience your user interface and play with your functionality to see how well it fits.

But don't expect anyone to start uploading their data into your software without assurances about its safety.

✔ Download an app

Gigaom forecast that EU developers will take in $85.3 billion in revenue in 2018. Hardly surprising when research from comScore shows that we now spend more time in apps on our mobile devices than we do on the web on desktops.

As the Symantec Internet Security Threat Report points out though, criminals will 'repackage malicious code within legitimate apps', or 'create new malicious apps that pretend to contain some useful functionality.'

Using secure code signing and legitimate stores is essential for keeping your customers safe.

✔ Get information about your company or products

'While online research plays a bigger role throughout the major purchase process, 60 percent of consumers start by visiting a search engine, then go to the retailer's website,' says Toni White, CMO of GE Capital's retail finance business.

Even if customers aren't going to actively interact with you on your website, they are developing an opinion of you based on how you present yourself, including your stance on security.

✔ Get in touch

Research by Forrester found 44 percent of online consumers say that having questions answered by a live person while in the middle of an online purchase is one of the most important features a website can offer.

Online help desks and contact forms all help you meet and exceed customer expectations, but they all involve the exchange of information and that has to be kept safe.

✔ Donate money (for example charities or crowd funding)

By 2016 the crowdfunding industry is on track to account for more funding than venture capital, according to a recent report by Massolution. Reports saw $16 billion crowdfunded in 2014, with 2015 estimated to grow to over $34 billion. And as for charity fundraising, 1.4 billion people donated money in 2015.

It's not just ecommerce sites that need to provide reassurance to people thinking about handing over their precious card details.

✔ Share your content on social media

'Social proof is the concept that people will conform to the actions of others under the assumption that those actions are reflective of the correct behavior,' says Ed Hallen of Buffer.

Social media sharing has huge and influential marketing potential, but people need to trust your site before they share it with their friends. They don't want to feel responsible for a colleague's crashed computer (or worse).

✔ Complete online banking transactions

Losses from online banking fraud rose by 48% in 2014 compared with 2013 as consumers increasingly conducted their financial affairs on the internet. But that doesn't mean you can ignore the online banking trend.

As Richard Levy, UK marketing director for MoneyGram says, 'Digital has raised the bar in terms of customer expectations as people get used to brands such as Amazon, and financial services needs to match these expectations.'

Get a head start this year

Say you've decided to take up running this year. You'll have a much better chance of seeing it through if you make a firm commitment. Signing up for and training towards a half-marathon in May is better than just saying 'I'll go for a run sometime'.

It's the same with your website. You need a target, a plan and you have to know what's coming up. While predicting the future is a fool's game, it doesn't mean we can't pick up a few pointers from the past.

Two major security issues of 2014, Heartbleed and Shellshock, exploited vulnerabilities in the open-source software that forms the foundation of ecommerce and online security. As Anthony Caruana of CSO Online says, 'Perhaps the biggest lesson from Heartbleed is that we can no longer trust something just because it hasn't been exploited yet.'

There are no safe assumptions in website security anymore. Being fit and resilient enough to tackle the unexpected should be your main motivation in 2016.

Better security creates opportunities too. In 2014 Google announced it would boost the ranking of sites that implement HTTPS across their entire sites, rather than just on transaction pages: a security best practice referred to as Always-on SSL. Google also favours sites that provide a good customer experience. So, keep visitors safe and you'll boost your search engine ranking: it's a win-win.

Cybercriminals will put your willpower to the test

No New Year's resolution is easy and, when it comes to your website, cybercriminals will do all they can to undermine your best intentions to keep your site healthy. These are some of the most common ways criminals can exploit an unhealthy website:

✔ Spoofing

A common criminal tactic is to clone a popular website and trick people into entering passwords or other confidential information. This is why verifying your business-identity with Extended Validation SSL certificates is so important: that green address bar could be the only thing distinguishing your site from its malicious clone.

✔ Data capture

The kind of malware that criminals attempt to inject on to your site can do a range of things. Sometimes the aim is to infect visitors' computers so they can log keystrokes and steal other personal information. Other times criminals may want to infiltrate your server and network. Remember, the more company data you have on the same network as your web server, the more the criminals can steal.

✔ Watering hole attacks

Hackers might be targeting your customers with a view to infecting them with malware. This kind of 'watering hole' attack exploits the popularity of legitimate sites like yours by injecting malware into the software that runs them. This software then infects site visitors. Watering hole attacks are nasty and deliberately designed to go undetected.

Your recommendations for a healthy website in 2016

✔ Control access to servers and certificates:

If you are a large company, with multiple web servers and SSL certificates, there are more people with access to sensitive website security information, meaning a higher risk of insider threats.

Minimise the risk posed by rogue employees: control access to systems and servers and regularly update passwords, especially when there is any personnel change in the website security management team. Ensure that you also have processes and policies in place to restrict access, log changes and protect private cryptography keys.

✔ Set up a trust or safety centre on your site:

Prove to website visitors that you take their safety seriously by setting up a page on your site to explain what security steps you take, and what that means for them.

The UK retailer, John Lewis, sets a good example. Tell visitors what you encrypt and how, and provide accurate assurances. Not only are you helping your customers be more secure but this kind of security advice shows that you take security seriously.

✔ Deploy Trust Marks:

People are trained to look for visual clues about the safety of your website. For example, 64 percent of respondents to an international online consumer study conducted in September 2015 were more likely to continue online transactions if they saw the Norton Secured Seal.

Give visitors what they want. The Norton Secured Seal, which you can display when you purchase Symantec's SSL certificates, is the most recognised trust mark on the internet and is viewed over a billion times a day in 170 countries.

✔ Choose a reputable Certificate Authority:

Different certificate authorities (CAs) have different levels of rigor, resources and resilience when it comes to fighting cybercrime.

It's important to remember that your choice of CA does matter. Not all Secure Sockets Layer (SSL) certificates are issued with equal diligence and businesses should consider the level and thoroughness of authentication and security that goes into the SSL certificates in which you place the trust of your brand and your customers.

Not all SSL is the same because not all CAs are the same. CAs that follow established best practices for securing private keys, along with vigilant enforcement of stringent authentication practices, are critical components in keeping the Internet a safe environment for all.

Founded as VeriSign in 1995, Symantec supports the world's largest and most critical certificate deployments.

- Symantec's validation services process on average over four and a half billion hits per day – with zero downtime in over 8 years.
- 97 of the world's 100 largest financial institutions and 75 percent of the 500 biggest e-commerce sites in North America use SSL Certificates from Symantec.
- Symantec's robust PKI infrastructure includes military grade data centers and disaster recovery sites for unsurpassed customer data protection, availability, and peace of mind.

✔ Stay on top of SSL certificate renewal dates:

Miss an SSL certificate renewal date and visitors will see a security warning. And that's bad for business: in a US online consumer study, 91 percent of respondents will not continue if they see a browser warning page indicating the absence of a secure connection.

Have someone in charge of renewals and use a dedicated tool to monitor and manage your certificates. Symantec offers a range of SSL management tools, to match your size and certificate needs.

✔ Get staff into good habits:

Symantec research conducted with the Ponemon Institute says that 51 percent of employees claim it's acceptable to transfer corporate data to their personal computers, as their organisations don't strictly enforce data security policies.

It's not just how you collect customer data on your website that matters, it's also how you store and use that data. Employees need to know how to stay on the right side of compliance. The EU data protection directive is a good place to start.

✔ Make sure employees don't fall off the wagon:

You have to keep your website safe from threats inside and out.

Educate employees about the risks of cybercriminals gaining access to webservers via a network infection originating from malicious emails, websites or social engineering tactics on social media.

Symantec offers free online resources as well as instructor-led training and certification.

✔ Educate yourself:

Don't underestimate the power of knowledge. Getting yourself in shape will help you better support your site. And while understanding all the technical ins and outs may not be possible, understanding what threats you face is crucial.

In other words, it's good to partner with a security expert like Symantec, but you also need to know why you need a security partner in the first place.

✔ Run malware scans:

'The fact that hacktivism and malicious software have been around for some time doesn't mean they're less threatening and we can relax – quite the opposite,' says the Information Security Forum in its Threat Horizon 2015.

Criminals want to spread malicious software, and they'll try to use your legitimate site to do so. So start running regular health scans, and make sure you don't miss any malaise. Malware scanning checks your public-facing pages to help protect your business and customers. Daily website malware scans are included with all Symantec SSL certificates.

✔ Run vulnerability scans:

Cyber criminals are looking for a way into your website and according to Symantec's Website Security Threat Report, a lot of you are making it easy: in 2014, 76 percent of legitimate websites had a critical vulnerability.

Assess your website's immune system – many of Symantec's SSL certificates include free vulnerability scanning – and attend to your deficiencies.

✔ Keep your servers up to date:

Over two thirds of websites used to distribute malware are legitimate, compromised websites according to Symantec's research. The problem is, a lot of businesses don't keep their server software up to date.

If a patch or update is released, it means the software manufacturer has developed a cure for a particular vulnerability. So, if you don't keep your servers up to date, you are putting your site at unnecessary risk from a whole back catalogue of vulnerabilities, making it much easier to exploit.

Keep your site's vulnerability to a minimum: whenever a patch is released, test and install it immediately.

✔ Use Extended Validation SSL certificates:

Prove you are who you say you are with Extended Validation (EV) SSL certificates. These turn a visitor's address bar green and tell them that you've been through a rigorous business-identity check. In fact, the EV SSL bar increases the feeling of security for 60 percent of shoppers according to a Symantec online consumer study.

After deploying Symantec Secure Site Pro with EV SSL Certificates, Liberty Games – an online retailer selling equipment ranging from £5 to £35,000 – saw a boost in revenue of over 35 percent year over year.

✔ Implement Always-on SSL:

By implementing HTTPS across your entire site, with SSL certificates from a trusted certificate authority such as Symantec, you encrypt all visitor interactions with your website – not just login pages and shopping carts.

This basic, easy-to-implement security measure delivers authentication of the identity of the website and encrypts all information shared between the website and a user (including any cookies exchanged), protecting the data from unauthorised viewing, tampering or use.

As we explain on our blog, protecting login and transaction areas alone doesn't prevent hackers from stealing the cookies that store a user's session and using them to recreate a website session and gain access to all kinds of sensitive data.

That's why the Online Trust Alliance is calling for all websites to adopt what's called Always-on SSL and many major names have already adopted the practice, including Google, Facebook and PayPal: it's time you did too.

Now you know what you need to do to get your website into peak condition, but what to do first?

The easiest thing is to get in touch with someone from Symantec, call **0800 032 2101** or **+44 (0) 208 6000 740**. After all, we're the specialists when it comes website security healthcare: that's why 93 percent of the Fortune 500 and 97 of the top 100 US banks worldwide are using our products.

Symantec | Website Security Solutions

For specific country offices and contact numbers, please visit our website. For product information in the UK,
Call: 0800 032 2101
or +44 (0) 208 6000 740

Symantec (UK) Limited
350 Brook Drive,
Green Park, Reading,
Berkshire, RG2 6UH, UK.
www.symantec.co.uk/ssl

Simple Steps to a Secure Website in 2016