Top 3 Website Security Myths Revealed

Learn the Facts So You Can Make Smart Website Security Decisions
Top 3 Website Security Myths Revealed

With the many falsehoods and myths surrounding website security, how do you sort through what’s true so you can choose the right protection to keep your business, website and customers secure?

In this paper, we will take a look at the top 3 website security myths—and give you the real facts—so you can make informed decisions about the kind of protection you truly need.

1. Hacking? It won’t happen to me! My business is too small.
Hackers don’t discriminate—and the threat is real. In fact, cybercriminals increasingly target smaller businesses, with three out of five attacks last year targeting small and medium-sized organizations.¹ According to one study, 55 percent of small businesses have experienced a cyberattack in the last 12 months.²

Why your small or medium business is a hacking target
Often due to budget constraints, smaller businesses tend to have fewer security safeguards in place than larger enterprises because they lack the necessary resources, security expertise and technologies to stay protected. As a result, the last five years have shown a steady increase in attacks targeting businesses with fewer than 250 employees.³

A small business cyberattack will cost you
It is difficult to estimate your risk and the costs of a security breach. One study cited that 60% of small companies that suffer a cyberattack are out of business within six months.⁴

The direct cost following an attack might include the cost for experts (for example legal IT, PR or risk consultants), but also includes productivity losses, and lost sales. The average cost of a small or medium business data breach in 2016 was $36,000.⁵

Take a risk-managed approach to security
A thoughtful approach to website security is vital and you must create a plan that is based on knowing what your risks truly are, and then take the steps necessary to prevent those risks from becoming a danger to your business, customers and website. Thoroughly assessing your threat risk may require involving multiple stakeholders or enlisting outside help if you are a small business with limited internal resources.

2. I don’t store my customers’ credit card data, so I don’t need SSL/TLS.
Even if you don’t store credit card data, browsers have now begun notifying visitors of non-HTTPS websites that don’t have SSL/TLS. Any website without an SSL/TLS certificate will be marked by browsers as "not secure."

To prevent website abandonment and visitor mistrust due to customer security fears, encrypt your site with an SSL/TLS certificate.

Additionally, if you collect any personal details such as logins, email addresses, names or phone numbers, and you do not have an SSL/TLS certificate, any of that information can be intercepted by hackers.

In 2015, 3 out of 5 attacks targeted small and medium-sized organizations.¹

SSL/TLS Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates provide validation that a website is who it claims to be and thus offer customers an assurance that they can trust you. SSL/TLS certificates are issued by independent, trusted third-party companies, like Symantec, known as Certificate Authorities (CA).
SSL isn't only about security—it's also about trust
Online consumers are getting savvier about knowing how to spot signs of safety on a website, and browsers are now helping. Popular browsers have now begun to visually indicate the “Not Secure” status of sites that don’t have the right level of SSL encryption, giving consumers an easy way to know if they want to go to your site, or stay away.

Give visitors security and peace of mind
SSL certificates are the most proven, reliable and scalable method to protect web transactions and sensitive information, and reassure visitors that your site is safe.

The Symantec Norton Secured Seal that comes with Symantec SSL gives your website instant credibility by visually reassuring customers that your site’s identity has been verified and is secured with SSL—while also keeping your site from being flagged as “Not Secure” by browsers.

Opt for an SSL certificate with Extended Validation (EV)
When you select an SSL certificate, aim for the highest level of protection for your site visitors, especially if you handle sensitive customer information.

The last 5 years have shown an increase in attacks targeting businesses with <250 employees.

EV certificates are validated to the meticulous guiding principles set by the CA/B Forum, providing the highest levels of security and trust to consumers. The assurances EV provides put customers at ease to purchase more—and more often. Be sure to choose an EV SSL from a globally recognized certificate authority, and consider whether or not the CA also offers malware and vulnerability scanning, or warranties or “insurance” to cover you if something does happen.

SSL certificates are the most proven, reliable and scalable method to protect web transactions.

Implement Always-On SSL
Many businesses use the SSL/TLS protocol to encrypt their login pages—but fail to encrypt subsequent pages within the user’s session. Single-page use of SSL/TLS won’t keep users safe in the face of today’s increasing threats.

Always-On SSL is a fundamental, cost-effective security strategy that helps protect every page of your website.

3. I would know if my website was in danger.
A website’s security is less about what you can see and more about what lies beneath. Hackers are always searching for sites to invade, and probably have already probed your systems, checked out your software and are ready to take advantage of any unknown security holes you may have.

Your website can have hidden vulnerabilities
Your website may not have any value to hackers on the outside, but the underlying SQL database on your server can be fertile ground for hackers who want to gather identity theft information. Websites can easily contain vulnerabilities or potential entry points that allow hackers to damage data, change functionalities, or allow code and data to be downloaded or manipulated.
This is a serious issue for businesses because major search engines scan websites and will blacklist any website that is found with malware, which results in reduced (or no) traffic, and decreased business.

**Act as if your website is always being probed**

In order to stay aware of what is happening behind the scenes on your website, regular malware scans are critical. Symantec offers daily scans for malware (to see if someone has tampered with your website code) and deeper automatic scans to find if your website is open to any potential vulnerabilities. Once you know your site has vulnerabilities, you can fix them, rather than leaving your business and customer information available to the hackers.

**Symantec offers superior encryption that's 64,000x stronger than industry standard (RSA) certificates.**

**Build a comprehensive security strategy**

To ensure you are doing all you can to keep your website safe, you must strengthen your security measures comprehensively—including your overall defenses, business policies, practices and procedures—with products from reputable website security authorities, like Symantec.

**Why Symantec?**

Here are just a few reasons to choose Symantec:

- **Reputation**: When you choose Symantec, your site displays the Norton Secured Seal—the most recognized trust mark on the web—giving visitors confidence in your business and your site. Symantec displays over 1 billion trust seals daily.
- **Trustworthiness**: Symantec secures the world’s top companies, including more than 90 percent of the Fortune 500, and is a longstanding, reputable market leader.⁵
- **Encryption**: Symantec offers superior encryption that’s 64,000 times stronger than industry standard (RSA) certificates, with daily malware scans, vulnerability assessments, warranty protection and installation tools to automate SSL Assist Plus.⁷
- **Authentication**: Multi-layered security makes our certificate issuance and authentication processes the most rigorous in the industry.
- **Expert Advisors and Support**: We are present 24 hours a day, 7 days a week. Symantec continues to earn near-perfect scores for our customer service worldwide.⁸

To learn more about how to protect your data in transit with an SSL certificate from Symantec, contact us today.

**Contact our sales advisors:**

- **Via phone**
  U.S. toll-free: 1-866-893-6565

- **Visit our website at**
  www.symantec.com/ssl

---

1. [http://www.forbes.com/sites/centurylink/2015/06/11/is-your-small-business-a-perfect-target-for-hackers/#64aea8d313a0](http://www.forbes.com/sites/centurylink/2015/06/11/is-your-small-business-a-perfect-target-for-hackers/#64aea8d313a0)
6. Internal customer analysis, October 2015 against Fortune 500 2015 list.
For global offices and contact numbers, please visit our website.

For product information in the U.S., call:
1-866-893-6565 or 1-520-477-3111

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/ssl

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne, 3004
ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

For product information in the Americas (Non-U.S.), call:
Mexico: 554 738 0448
Brazil: 800 038 0598

For product information in the U.K., 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

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929
Germany: 0800 128 1000
France: 0800 90 43 51
Spain: 900 93 1298

Follow Us: