
thawte
TOP
10
WEBSITE SECURITY MYTHS REVEALED

INTRODUCTION

Many companies fail to put in place the most fundamental protections to keep themselves safe. The problem is that many businesses have steeped themselves in the mythology that surrounds website security and bury their heads when it comes to the dangers that EVERY business faces.

To be truly safe, they need to move from ‘myth’ to ‘reality’, shoring up their defences, corporate policies, practices and procedures to the point where they can honestly say: “There is no more I can do” – and then look again and do even more.

So, let’s take a look at those myths and where they fall down.

MYTH 1

Hacking?

It won't happen to me!

Many believe their website is such a small fish in the Internet Ocean that no hackers would even take a look at. The problem is that they are now casting their net very wide indeed.

Assume your website is always being probed

If you assume your website is always being probed by hackers using scripts, you will be close to the truth. Perhaps your website really doesn't have any value – but maybe the underlying SQL database on your server is fertile ground for identity theft information.

Your SQL database could be fertile ground for ID theft

The more subtle risk to any website hack is the changes the hacker might make to your site without your knowledge. 'Spear phishing' is another line of attack that online criminals are now executing, this is where they seek to gain unauthorised access to sensitive data using faked - but highly credible - emails impersonating a colleague or perhaps a bank in order to trick targets into sharing personal data and also corporate and highly sensitive information.

The size of your business does not matter

But whatever you do, do not believe the size of your business makes a difference to the hackers. The sharks have you on their radar, however big – or small – you might be.

MYTH 2

Security risks can be quantified

This is the ‘rule of thumb’ myth. Trying to quantify such risks is all but impossible. How, for example, can you know how much it might cost you, if your website was hacked or your network badly infected?

How can you measure the impact on your business?

What price would you put upon sensitive corporate or customer data falling into the wrong hands? How can you measure the impact on your business and how long it would be before you were back up and running? And what long-term price could anyone set against a breach leaving customers taking their business elsewhere?

A business needs a measure of how secure it is

Every business needs some measure of how secure it really is, and the best approach is to build security programs from the ground up so you have a comprehensive view of your ‘estate’ and the ability to identify the security strategies and systems most suited to your needs.

3

MYTH 3

Looking after **security practices?** That's the CISO's job

The Chief Information Security Officer should be the senior-level executive responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected. But should it be their sole responsibility to define and enforce security practices?

Unloading responsibility onto one person is not a good idea

A company should build an information security strategy and process around the specific needs of the business – and that means involving a multitude of people and departments across the organisation.

Information Security is no longer solely a technical problem

Information Security is no longer solely a technical problem, but encompasses management of people, process, legal affairs, risk management, public relations, physical security, organisational change and many other areas, alongside technical management of the threat.

A risk-managed approach is critical

It is also now clear that, with such a complex threat landscape, a risk-managed approach to Information Security is vital. The assessment of such risk requires the involvement of many stakeholders across the business and, critically, an individual to manage this process, who might well be the CISO.

MYTH 4

SSL is broken

4

In some quarters, the argument has been going around that the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) system is broken. Many of the anti-SSL camp believe the time has come to replace SSL with a new system. Some have even argued that Certification Authorities (CAs) themselves should be done away with.

Failures due to lack of internal security at end-entity level

This argument rides roughshod over all of the benefits that SSL has delivered for so long. SSL certificates are widely acknowledged as the world's most dependable and scalable cryptographic system, so why are the daggers suddenly out? There have been high-profile security failures involving SSL of late. But the reality is that these were often due to a lack of appropriate internal security controls at the end-entity level, rather than a system-wide failure.

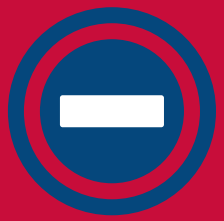
SSL is not broken – it's a key part of any defence strategy

SSL certificates have proved to be a major factor in Internet security for the best part of two decades and are still by far the most proven, reliable and scalable method to protect web transactions. The reality is that SSL is not broken - but very much a key part of any defence strategy.

MYTH 5

I don't store credit card data, **so I don't need SSL**

That doesn’t automatically make you or your customers safe. There are many ways cyber attackers can wreak damage on your organisation and reputation.



You need the highest levels of protection

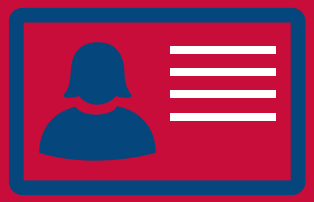
You need to have the highest levels of protection in place to keep hackers at bay. This means having safe areas for your customers where they know they are out of harm's way, as well as operating the highest levels of security for log-ins and passwords.

Secure areas

These are interactive and personalised website ‘portals’ providing customers with online access to sensitive information in a secure environment. This can be restricted to users with electronic certificates, enforcing another powerful layer of security

Log-ins/Passwords

Anyone logging in to your site should be using passwords that are at least 10 characters long and contain multiple character types, including lowercase, uppercase, numbers and special characters. Login information should always be unique and never reused across multiple web sites.



Personal details

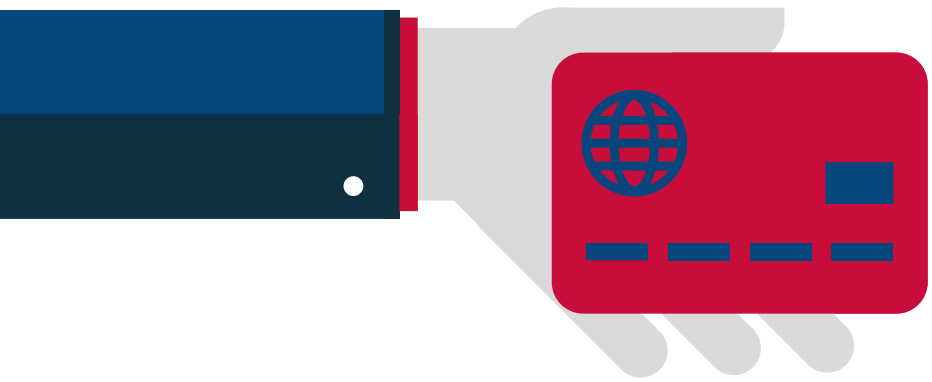
Such as names, email address, contact numbers and mailing addresses. If you collect personal data, identity theft may become a plausible threat to customers. Take the necessary precautions; otherwise it can be devastating to your customer and your reputation. Increasingly, customers are educated online shoppers and won’t buy if you don’t have an SSL certificate.

Even if you don’t sell online, customers will appreciate care taken to protect personal data

MYTH 6

All types of certificates **issued by a CA** are the same, aren't they?

No, they are not. There are several types of certificates on offer – and not all can be trusted to the same degree.



Domain Validated (DV)

The lowest cost means of securing a website, this does not provide authentication or validation of the business behind the website.

Organisation Validation (OV)

These certificates include full business and company validation from a certificate authority using currently established and accepted manual vetting processes, but are not validated to the highest standards set by the CA/B Forum*.

Extended Validation (EV)

Fully validated to the meticulous guiding principles set by the CA/B Forum*, providing the highest levels of security and trust to end users. The entire address bar will turn green for ‘safe’.

* CA/B Forum, an independent standards body that requires in-depth verification of the legality and probity of a company before it is issued with a certificate

Opt for an SSL certificate with EV from a globally recognised CA

Always opt for an SSL certificate with EV from a globally recognised certificate authority, such as Thawte. These certificates guarantee the business is legitimate, whereas many other types only validate the domain, not its owners and operators.

Add the seal of assurance

Trust marks/seals are another important means to reassure customers that it is safe to shop on a site. The Thawte Trusted Site Seal gives your website instant credibility in the online world by visually reassuring customers that your site's identity has been verified and secured with SSL.

MYTH 7

Only shady-looking websites are really dangerous. **Mine's safe and secure**

It's a given that, however much money, time and technology you have, your website will never be 100% secure. Don't imagine what looks okay is okay. It's all about what lies beneath.

Hackers are constantly seeking out and discovering security flaws

The time between these discoveries and the required patch software will make you highly susceptible to a full-on assault. One thing you need to be aware of is that hackers have already probed your systems, checked out your software and are ready to take advantage of any zero-day vulnerabilities that might open you up.

Software is inherently flawed

Even the simplest websites rely on software - software is inherently flawed and contains errors or bugs. You should know the components your website relies on to operate and keep tabs on the known issues, and releases of updates and patches.

The harder you make it, the more likely they will move on

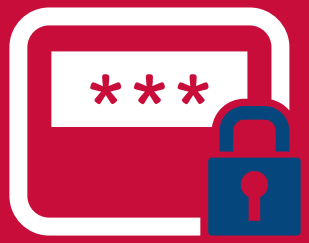
Even though total website security is a myth, the goal should be to make yours as secure as possible. Attackers are opportunists, and the harder you make it for them, the more likely they will move on and find a site that is not as robust as yours.

MYTH 8

I don't need SSL on all my web pages

8

Many organisations use the SSL/TLS (Secure Socket Layer/ Transport Layer Security) protocol to encrypt the authentication process when users log in – but fail to encrypt subsequent pages during the user's session. This is not good practice, because intermittent use of SSL won't keep users safe in the face of today's burgeoning threats.



People are spending more time logged in

People now spend more time logged in, and this has seen a surge in cybercriminals targeting consumers using a method called ‘sidejacking’. This takes advantage of consumers visiting unencrypted HTTP web pages after they have logged in and allows hackers to intercept cookies (typically used to retain user specific information such as username, password and session data) when transmitted without the continuous protection of SSL encryption.

Any company serious about protecting customers will implement Always On SSL

You need end-to-end security that can help protect every web page your users visit. ‘Always On SSL’ is a fundamental, cost-effective security measure for websites that helps protect the entire user experience from start to finish. It is supported as best practice by leading industry players such as Google, Microsoft, PayPal, Symantec, Facebook and Twitter. Any company serious about protecting their customers and their reputation will follow their lead and implement Always On SSL, with SSL certificates from a trusted Certificate Authority.

MYTH 9

I have great anti-virus software on my network, **so my systems are safe**

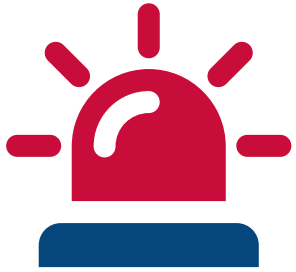
Your anti-virus software may well be excellent – but that isn't enough. Anyone who thinks AV is still all they need is, quite bluntly, living in the past. The world has changed and attackers (and malware threats) have moved on, with far too many variants for traditional signature-based anti-virus products to cope.

However good your AV might be, they will target a weakness

As always, while security vendors, IT administrators and end users adapt new measures to block security threats, attackers are constantly creating new, sophisticated ways to get through their defences. However good your AV might be, they will target a weakness in the system, network – or indeed end users themselves – in their mission to break through.

AV products used as sole or main means of defence are increasingly failing

With ‘brute force’ threats designed to target different weaknesses on different systems, never using the same technique twice, it’s no surprise that AV products, used as the sole or main means of defence, are increasingly failing, causing costly downtime, clean-up efforts and data loss.



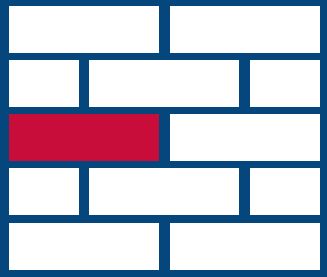
AV only is not enough - companies need comprehensive attack prevention

A successful attack can now be the passport to significant revenue streams, and the resources and skills employed to undermine security defences are formidable, so you can be certain that the tenacity and guile of the cybercriminals will only increase, too. For all of these reasons, the era of AV-only is over. Companies need comprehensive attack prevention that integrates the full range of security technologies.

MYTH 10

We use a firewall, so we're well protected against attacks.

This is a myth still rife across many corporations and seems to be based more on some 'feel good' fantasy than fact.

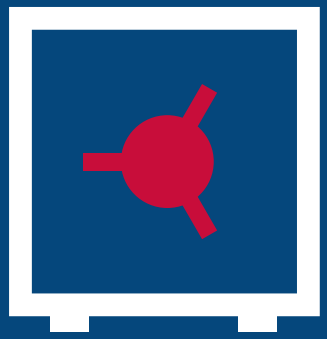


Firewalls need to be thought of as a temporary fix rather than a permanent repair

Firewalls are of real value and will certainly control traffic. But that server will need to see web requests, so these cannot be filtered. Equally, web application firewalls can assist in protecting known vulnerabilities and unusual traffic, but cannot normally provide protection against business logic vulnerabilities, custom code vulnerabilities, valid use that corrupts data and zero day attacks. And while they can be useful in temporarily filtering traffic when a vulnerability is discovered, they need to be thought of as a temporary fix, rather than a permanent repair.

SQL injections can bypass typical login firewalls

SQL injections are one the most potent threats to computer security and notoriously hard to detect. The most effective injections wreak havoc on website security because they can bypass typical login firewalls and send SQL queries to formerly protected databases.



Organisations need to utilise more comprehensive security measures

What's the answer? Organisations need to utilise more comprehensive security measures that can offer support from data leaks – and awareness, where a threat or system breach occurs. In fact, beyond singular reliance on a firewall, technologies for perimeter protection are essential to deliver an effective layered defence strategy around security management.

WHY THAWTE?

Protect data in transit with an SSL certificate from Thawte today.

Not All SSL Is the Same, We make SSL our business in order to protect yours. Thawte online security is trusted by millions of people around the world. Here are just a few reasons to switch to Thawte:

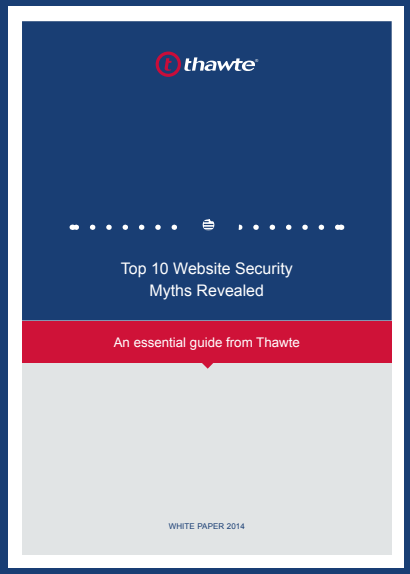
High- assurance digital certificates
Global reputation for uncompromised reliability
Up to 256-bit SSL encryption
World-class, multilingual support
New, lower prices that are within your security budget
Thawte Trusted Site seal

Protect your data, safeguard your business, and translate trust to your customers with high-assurance, digital certificates from Thawte.

BUY TRY LEARN MORE

thawte®

READ OUR FULL WHITEPAPER TO GET ALL THE FACTS



DOWNLOAD WHITE PAPER