



THE BRAND BULLETIN

Calling All Fraudsters

How lapsed SSL certificates expose your business—and what you can do about them



Does your business extend regular invitations to criminals? You might be surprised at how many organisations do. While nearly every company with an online presence these days uses SSL certificates to keep valuable data safe, most of them are not good at keeping them up-to-date.

SSL certificates are part of everyday online life, their reassuring presence revealed by the 'https' prefix or the green address bar that tells you a website is safe. Yet they can be tricky to manage. When SSL certificates

lapse, the door is open for fraudsters to help themselves to personal information and credit card details, and to listen in on your confidential discussions. If renewals go wrong, the consequences can damage your brand. In the sections below, we explain in clear terms how organisations can keep their online properties—and their customers—safe.

The problem is that SSL certificates need to be regularly renewed, typically every one to three years. And unlike domain names, renewal is not a simple matter of making a payment. Each time SSL certificates are reissued, through a process called Domain Control Validation,

SSL certificates: the 30-second introduction

SSL certificates encrypt session information and assure users that they are visiting a legitimate, trusted website. They establish a protocol for secure communications between client and server.

- Extended Validation Certificates offer the highest levels of encryption, security and trust. They are recommended for all online businesses and feature the reassuring green address bar.

- Premium Certificates include full business and company validation, and provide higher levels of trust than domain-only SSL certificates, but lack the green address bar.
- Wildcard Certificates secure unlimited subdomains on a single certificate, removing the need to manage and track individual certificates.
- UCC/SAN Certificates can contain up to 200 domain names in a single certificate.

To offer an analogy with the physical world, it's as if security at any of your facilities, anywhere around the globe, could become instantly compromised at any time. Arguably, **the consequences are worse online**, where trust is your most valuable currency.

their owners must prove they are the rightful owners of the domain name to which the certificates apply. To add further stress to the process, there is usually a limited window of time in which to renew a SSL certificate.

If you only have one or two domain names and don't deal with sensitive data like client login details or credit card information, this might not be a problem. Indeed you may not even need a SSL certificate.

Essential—but hard to handle

But most organisations do. Many use websites for e-commerce, or have large numbers of registered users. Others are sensitive to casual visitors' concerns about security: with cybercrime on the rise, people need assurance that they're not being compromised when using a website. Increasingly, companies are applying SSL certificates to their basic websites and using them for internal purposes, too.

Multiply this across several countries and a collection of domain names, and it's easy to see how SSL certificate management becomes a thorny issue for medium to large organisations.

To offer an analogy with the physical world, it's as if security at any of your facilities, anywhere around the globe, could become instantly compromised at any time.

Arguably, the consequences are worse online, where trust is your most valuable currency. When an online retailer serves up a security error message, for example, the brand damage is immediate and visible everywhere. And your competitors are only a click away.

Even top brands and experts slip up

Last summer, a researcher uncovered security flaws at one of UK's retail giants, including inconsistent use of SSL certificates across its site. The result was widespread negative publicity and scrutiny from the Information Commissioner's office—at a time when the company was looking to build out its e-commerce operation.

Nor are the experts immune. The UK's internal security agency, MI5, suffered a brief but reputation-damaging website glitch in April 2012 when it was late in replacing an expired certificate*. Also last year, the website for Sage Pay, a business payment service, presented users with a "This connection is untrusted" error message when the company experienced a delay updating an SSL certificate.

If even top brands and security experts are having problems managing SSL certificates, how is everyone else doing? Not well, as research carried out by CSC Digital Brand Services in February 2013 revealed. We

ADVERTISEMENT

DNS: Maintaining vital links

Your company's online presence is only as good as the infrastructure behind it.

CSC Digital Brand Services' enterprise-class Domain Name System (DNS) services offer the stability you expect and the security you need when servicing clients around the world, and will help bring success to your e-commerce efforts and other online strategies.

Our DNS services are provided through our partnership with VeriSign, which maintains the most robust DNS infrastructure on the planet. VeriSign is responsible for the .com and .net top-level domains (TLDs), the federally audited .gov TLD, and other critical extensions.

CSC Digital Brand Services puts the reliability and global distribution of the world's best DNS infrastructure on your side.

To learn more, visit www.cscglobal.co.uk or email us at DBServices@cscglobal.com

found that of the top 100,000 domains ranked by the web information firm Alexa, more than 4,500 had expired SSL certificates and over 150 were set to expire within seven days. What's more, over 25,000 had certificates that referenced an incorrect domain name. More than 800 of the certificates we found were MD5 certificates, which are particularly vulnerable to attack.

Most likely, many of these domains have been managed piecemeal. As CSC Digital Brand Services Product Expert Ken Schmid points out, "It's not unusual to find SSL renewals being handled by individuals who might then leave the company, taking all the relevant information with them. We also see different departments buying certificates from different vendors, creating lots of different lists of domains and certificates. Often, everything is just managed on a spreadsheet, or worse, several spreadsheets."

Centralisation is the key

The good news is that while digital signatures may seem complex, managing them is not. The key, according to Schmid, is centralisation. "Having a single overview


Certificate troubles in high places

CSC Digital Brand Services research conducted in February 2013 found that of the SSL certificates in use at the top 100,000 Alexa-ranked websites:

- **Over 25,000 referenced the wrong domain name**
(Most browsers will confirm that a site's SSL certificate matches the name that is listed on it (and display a warning message when it doesn't). Often, for cost-cutting reasons, companies repurpose their existing SSL certificates for other sites, especially the more expensive EV certificates, thus creating name mismatches.)
- **More than 4,500 were expired**
- **More than 800 used a vulnerable certificate type**
- **Over 150 were due to expire within days**


Would you like more information?

Please email us at DBServices@cscglobal.com



Would
you like more
information?

Please email us at
DBServices@cscglobal.com



of all your SSL certificates is the most important step toward making sure you don't miss expiry deadlines, and avoiding duplication," he says. "And it has other advantages, too. You can also use this view to make sure each of your digital properties has the appropriate level of security. It also helps you to allocate costs correctly."

This centralisation also holds out the possibility for organisations to manage all of their digital assets—domains and social media profiles as well as certificates—in one place. That way, as companies grow or move into new markets with different rules, they can quickly assess how their digital assets measure up to potential risks.

Efficient validation is the other critical step, according

to Schmid. "Validation is an essential part of SSL certificate renewal," he says. "But it can take days for each certificate. For any organisation with more than a few certificates, this not only creates a major admin headache, it also increases the likelihood of missing renewal deadlines. It's important to streamline this part of the process as much as possible."

Reliable SSL certificate management

CSC Digital Brand Services recommends a simple, three-step approach to managing SSL certificates in a secure and cost-effective way:

1. **Analyse** your certificates and domain names to find out what SSL certificates you own and how much they are costing you.
2. **Consolidate** your portfolio of certificates so registration, renewal and verification can all be managed from one place.
3. **Develop** a policy as you would for domain names or social media accounts so you can manage certificates efficiently on a continuing basis.

About CSC Digital Brand Services:

Founded in 1899, Corporation Service Company® (CSC®) provides business, legal and financial services to many of the world's largest companies, law firms and financial institutions. An ICANN-accredited domain name registrar since 1999, CSC Digital Brand Services is the trusted partner of more than half the 100 Best Global Brands (Interbrand®) and the customer approval leader for domain name services (*World Trademark Review*, 2010). CSC Digital Brand Services has an end-to-end solution for every brand protection need, from strategic domain registration and online monitoring to SSL certificates and trademark screening.

Visit www.cscglobal.com today to learn more.

Missed an issue? Download your copy of *The Brand Bulletin*, issue 5 today by visiting: www.cscglobal.com/brandbulletinuk

(* http://www.theregister.co.uk/2012/04/16/mi5_digi_cert_snafu/)