
30TH JULY 2019 12:52PM

CYBERSECURITY (HTTPS://WWW.VERDICT.CO.UK/CATEGORY/BUSINESS/CYBERSECURITY/)

# SSL certificates aren't enough – businesses need extended validation to prove legitimacy

Luke Christou (https://www.verdict.co.uk/author/luke-christou/)

Luke is the deputy editor of Verdict. You can reach him at luke.christou@verdict.co.uk

SSL certificates provide internet users with the assurance that the website they're visiting is safe, secure and under the control of a legitimate operator. Or at least it's supposed to.

A new study conducted by the Georgia Institute of Technology Cyber Forensics Innovation (CyFI) Laboratory, on behalf of leading certificate authority Sectigo, has found that basic SSL is not enough to guarantee the legitimacy of a website.


## The three types of SSL certificates

SSL (Secure Sockets Layer) certificates provide a secure channel between two internet-connected machines. This is commonly used to allow secure communication between a web server and web browser. URLs secured with SSL will start with HTTPS and a

POPULAR TODAY

(https://www.verdict.co.uk/robot-delivery-dog-continental/)

This robot delivery dog will hitch a ride in a driverless car to deliver your packages

lock will be displayed in the corner of the browser. Websites that are unsecured will display a “not secure” warning. The latter is often a good indication of a vulnerable or untrustworthy website.

Businesses can choose between three types of SSL certificates (https://community.digicert.com/en/blogs.entry.html/2014/08/11/types-of-ssl-certificateschoose-the-right-one.html) to protect their domains. Fundamentally, all three do the same thing. However, they offer varying levels of security.

## Domain validation

These domains are checked against the information provided when the domain was registered, usually by sending an email to the address provided in the WhoIs domain registry, or adding a file to the domain’s hosting server.

This kind of certificate only validates that the person requesting the certificate is in some way connected to the domain being certified, and offers little indication that the domain is being used for legitimate purposes or controlled by a legitimate organisation.



## Organisation validation

These domains are checked more thoroughly by the domain authority, who use business registry databases to verify the identity of the organisation or individual that has requested the certificate. In some cases the requesting party may be contacted to provide information that verifies their control of the site.

This is now the standard type of certificate used by public-facing websites, and are, for the most part, trusted as legitimate websites.

## Extended validation

These requests are stringently checked by the domain authority, which must follow government-issued standards to ensure that the person requesting the certificate has the right to do so.

(https://www.verdict.co.uk/robot-delivery-dog-continental/)


(https://www.verdict.co.uk/ai-in-the-fashion-industry-fit-ibm/)

AI takes root in the fashion industry with IBM partnership (https://www.verdict.co.uk/ai-in-the-fashion-industry-fit-ibm/)


(https://www.verdict.co.uk/m driverless-car-microsnap/)

Modular driverless car has swappable bodies for deliveries, taxi services and beyond (https://www.verdict.co.uk/mc driverless-car-microsnap/)


(https://www.verdict.co.uk/b stockpiling-prepare-for-brexit/)

Brexit stockpiling: The supplies you need to survive a no-deal Brexit (https://www.verdict.co.uk/bre stockpiling-prepare-for-brexit/)


(https://www.verdict.co.uk/te holidays-data-breach-customer-call/)

Exclusive: Teletext Holidays data breach exposes 212,000 customer call recordings (https://www.verdict.co.uk/tel holidays-data-breach-customer-call/)

Domains protected with extended validation (EV) will often display the name of the business operating the domain next to the URL in the browser, providing a clear indication that the URL is legitimate and under the control of the business it claims to be.

## Businesses must use extended validation to prove they're legitimate

While many internet users now associate the padlock in their browser with safety, a recent study by cybersecurity firm PhishLabs found that more than half of all phishing sites now use SSL certificates.

Likewise, past research has also uncovered thriving marketplaces for valid SSL certificates (https://www.verdict.co.uk/dark-web-ssl-certificates-sales/) on the dark web, where cybercriminals can purchase them for a few hundred dollars. Some of these certificates were issued by reputable authorities, and would allow cybercriminals to pose as a legitimate business based in the United States or United Kingdom.



## 3 Things That Will Change the World Today

However, while domain and organisation SSL certificates are fairly easy for malicious actors to get their hands on, the CyFI study found little evidence that EV certificates were being exploited by cybercriminals.

CyFI Lab cross-correlated a global repository of domains with EV certificates against a list of domains that had been flagged for suspicious activity, such as distributing malware to see how many of those blacklisted domains were using EV certification.

"Across the millions of domains with EV certificates that we studied, we found overwhelming evidence that EV certificates are highly indicative of a legitimate domain registered by a legitimate business," Brendan Saltaformaggio, director of the CyFI Lab and co-author of the study, said.

The study concluded that there is a 99.99% chance that a domain using an EV certificate is safe and not associated with any common form of cybercrime.

“Our findings reinforce the nation that consumers should view EV certificates as a browser security indicator for trusted domains,” Saltaformaggio said.

**Read more:** 25% of European banks could leave customers vulnerable to phishing (https://www.verdict.co.uk/online-banking-certificate/)