Changes to extended validation indicators put users at risk


Tim Callan


Chris Bailey

Tim Callan, Sectigo and Chris Bailey, Entrust Datacard

In 2019, both Google and Mozilla declared their intentions to remove distinctive extended validation (EV) certificate indicators from their browsers – indicators that tell consumers that a website has been vetted and validated through a thorough authentication process. At a time where the push towards increased consumer privacy exists on a global scale, with the US Congress proposing a handful of bills on the matter, and the General Data Protection Regulation (GDPR) taking effect in the European Union, these changes to Chrome and Firefox browsers seem to be a step in the opposite direction. Consumer privacy suffers in the absence of strong website identity.

Certificate Authorities (CAs) issue validation certificates in three standardised tiers: domain validated (DV) certificates, organisation validated (OV) certificates and extended validation (EV) certificates. DV certificates require the least amount of authentication and can be granted in a matter of hours, while EV certificates require the highest level of validation and can take weeks to complete.

DV certificates simply require validation that the website owner controls the domain in the certificate. The CA does not need to know the owner's identity, or to have any ability to contact the owner. To issue an OV certificate, a CA has the added requirement to verify the organisation's authenticity, name and address.[1]

Rigorous process

Websites that want to show users their confirmed identity go through the EV process when obtaining SSL/TLS certificates. The process involves multiple steps, modelled after banking 'know your customer' rules.[2] The process includes confirming that the organisation that controls the certificate's domain is duly incorporated and in good standing, taking steps to confirm that it is a legitimate business with an address and phone number, as well as confirming the authority of the person ordering the certificate. The confirmed identity is inserted into the EV certificate itself and is cryptographically signed, ensuring that it cannot be altered or imitated.

"Phishing on sites with EV certificates is rare. Phishers have migrated to encryption using anonymous DV certificates"

An EV certificate includes valuable identifying information on the organisation behind the website, such as the following from the EV certificate for the Bank of America.

```
CN = www.bankofamerica.com
SERIALNUMBER = 2927442
2.5.4.15 = Private Organisation
O = Bank of America Corporation
1.3.6.1.4.1.311.60.2.1.2 = Delaware
1.3.6.1.4.1.311.60.2.1.3 = US
L = Chicago
S = Illinois
C = US
```

This shows that Bank of America is a Delaware, US corporation, its Delaware corporate registry number, as well as the fact that Bank of America has a confirmed business location in Chicago. The information shows specific detail about the organisation that controls the Bank of America website, and gives open contact information and recourse, should anything malicious happen on the website.

Protect and reassure

The EV certificate validation process, standardised by Extended Validation Guidelines, ensures that all identity information in EV certificates is shown in the same way.[3] EV certificates protect consumers' private information, as well as the brands themselves from phishers.

Since 2009, browsers have distinguished websites that use EV certificates with a distinctive user interface (UI). This shows users that a website's owner has been strongly vetted and confirmed by a third-party CA. As such, phishing on sites with EV certificates is rare. Phishers have migrated to encryption using anonymous DV certificates.

However, Google Chrome and Mozilla Firefox decided to make changes to the EV UI in September 2019 and October 2019, respectively. Following these changes, users only see a website's URL, identical to what is shown for websites with simple DV certificate websites. Figure 1 shows the UI before the change in Google Chrome 76, and Figure 2 shows it after the change in Chrome 77.

Similarly, Figure 3 shows the address bar in Firefox 69, with both padlock icon and green text, as well as the name of the organisation. Figure 4 shows it in Firefox 70, after the changes to the UI.

Phishing on the rise

Historically, almost all phishing took place on unencrypted HTTP sites. These

websites received neutral UIs and phishers didn't need to spend time or money getting a certificate – even a DV certificate – that might link their identities to their scams. Over time, to avoid phishing scams, users learned to 'look for the lock' to increase their safety online.

Then, Google began posting warnings when users entered a non-secured site, which incentivised websites, even phishing websites, to move to encryption. Mozilla began posting similar warnings.

"To combat phishing scams, browsers can work together on common security indicators across devices. Browser companies can also engage CAs to create training schemes to help users protect themselves online"

Finally, Let's Encrypt began its practice of granting anonymous, automated DV certificates, including to known phishing websites. As such, nearly all phishing has moved to DV encrypted websites, which have the lock symbol that web users have been trained to spot and trust. Because of these automated DV certificates now being granted to malicious websites, the lock icon has lost its value. In fact, the FBI now advises web users to no longer trust the HTTPS or lock icon in browsers.[4]

Trustworthy sites

Research from RWTH Aachen University measured the rates of phishing sites among different certificate validation levels. The data showed that EV certificates accounted for 0.4% of total phishing websites with certificates, but 7% of the non-phishing websites. Websites with OV certificates accounted for 15% of phishing websites and for 35% of non-phishing websites. Let's Encrypt automated DV certificates made up 34% of phishing websites and only 17% of non-phishing websites.

A February 2019 study from the CA/Browser Forum corroborates these results. It shows that 0% of phishing sites have EV certificates, 4.15% of phishing sites have OV certificates, and 95.85% of phishing sites have DV certificates.

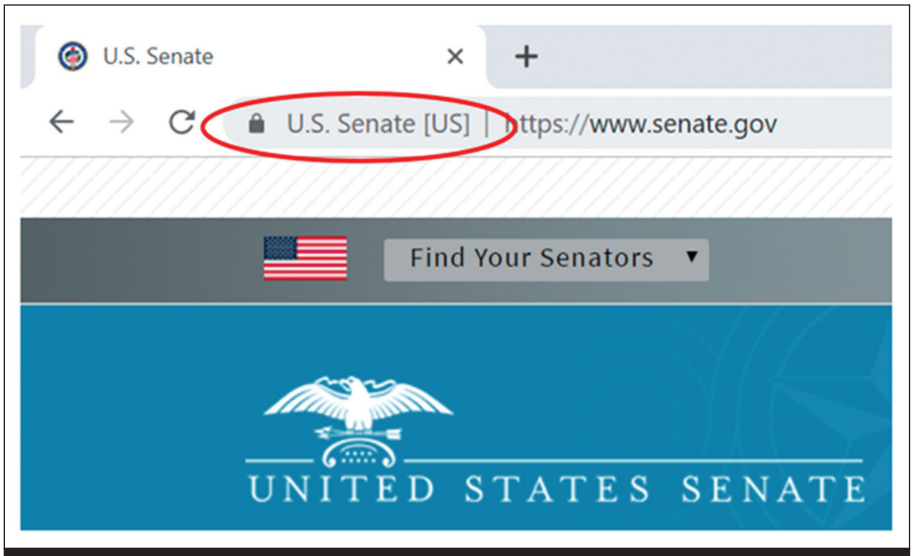


Figure 1: The distinctive EV user interface used in Google Chrome 76, showing a lock icon along with the owner of the website.

Figure 2: EV UI used in Google Chrome 76, showing a lock icon but not the owner of the website.

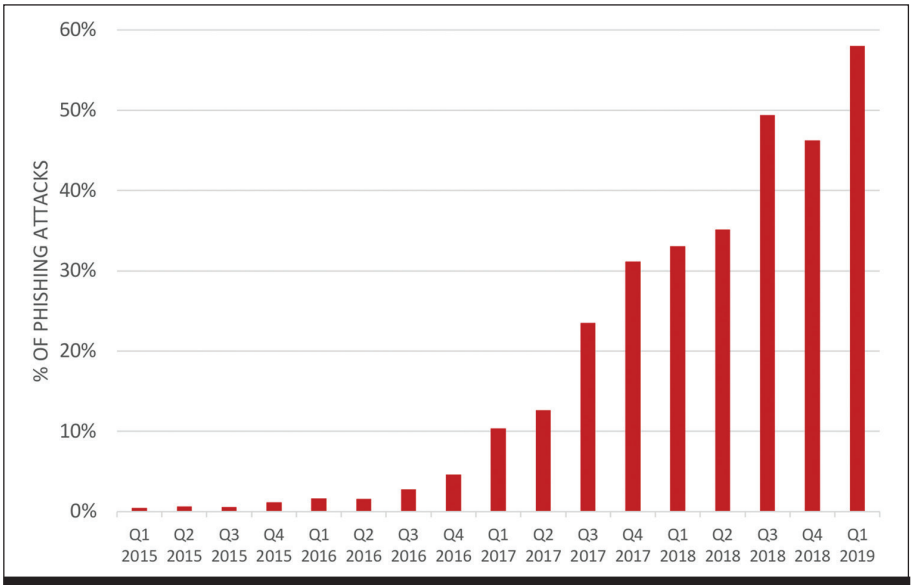
Figure 3: Distinctive EV UI used in Firefox 69, with lock icon and green text indicating EV authentication.

Figure 4: UI as used in Firefox 70, showing a lock icon but no green text indicating EV authentication.

Positive security indicators

We have established that the phishing risk on websites with EV certificates is miniscule, but with Google and Mozilla doing away with the UI that clearly tells Internet users whether the website they are using is safe, users will be forced to decipher this by the URL – which can be difficult to understand – and a possible interstitial warning from Chrome or Firefox warning visitors that the website they're about to visit is unsecured.

Reasoning for removing the EV UI from browsers includes the notion that users don't understand the organisation



The percentage of phishing attacks hosted on sites utilising HTTPS has steadily risen, in line with the wider deployment of SSL/TSL. Source: Drury and Meyer, RWTH Aachen University.

information that the UI displays and that, because of this, the EV UI isn't useful. However, rather than removing the UI and relying on a URL alone, an improved EV UI could help users understand more clearly whether the websites they visit are safe. Simple user training pop-ups within the browser can help users become savvier and more capable of protecting themselves from phishing scams.

"To combat phishing scams, browsers can work together on common security indicators across devices. Browser companies can also engage CAs to create training schemes to help users protect themselves online"

With industry standards and education, positive security indicators online can be as successful as they are in other areas. For example, most people expect to have a seatbelt available to use while riding in a car and feel uncomfortable and unsafe without it. Most miss this consistent and standardised security indicator when it is unavailable. The EV security indicator can be just as consistent, standardised and ubiquitous as the seat belt, if browsers and operating system vendors work in concert to make it a priority.

Phishers with EV certificates

One may ask, if Internet users do receive more information and become more educated and trusting of EV certificates, could phishers simply routinely obtain EV certificates? Yes, they could. However, once a phisher with an EV certificate uses it for a scam, the CA will quickly revoke the certificate as well as add both the guilty organisation's name and phishing domains to a flag list, making it impossible for the phisher to obtain another EV certificate from the same CA.

In addition, a common EV flag list for all CAs to share is being created to prevent phishers from obtaining EV certificates from other CAs once flagged by one.

Recommendations

When the EV requirements were initially created, the EV was intended to be an ongoing and evolving standard. While EV is not perfect, the data presented here indicate that EV helps protect Internet users from phishing scams and creates effective recourse for the rare times that phishing may occur.

Rather than removing EV certificate indicators, the industry should work together to improve them. To combat phishing scams, browsers can work together on common security indicators across devices. Browser companies can also engage CAs to create training schemes to help users protect themselves online.

About the authors

Chris Bailey is VP of trust services at Entrust Datacard. Previously he was the general manager of Trend Micro SSL, which was purchased by Entrust Datacard in 2016. Before that, Bailey served as the CEO and co-founder of the certification authority AffirmTrust, which was acquired by Trend Micro in 2011, and was co-founder and CTO of GeoTrust, a major world Certification Authority acquired by VeriSign in 2006. Bailey was a co-inventor of both the DV and EV SSL certificate.

As senior fellow, Tim Callan contributes to Sectigo's standards and practices, industry relations, product roadmap and go-to-market strategy. A founding member of the CA/Browser Forum, he has more than 20 years' experience as a product and strategic marketing leader for B2B software and SaaS companies, with 15 years' experience in the SSL and PKI technology spaces. Prior to Sectigo, Callan was vice-president of product marketing at Verisign, CMO of Melbourne IT Digital Brand Services, CMO of RetailNext and CMO of SLI Systems. He sat on the boards of directors for DigiCert and the Online Trust Alliance. His PKI and security podcast, Root Causes, is available on Spotify, iTunes, SoundCloud and other services.

Bailey and Callan are both members of the CA Security Council.

References

1. Drury, Vincent; Meyer, Ulrike. 'Certified Phishing: Taking a Look at Public key Certificates of Phishing Websites'. RWTH Aachen University, via Usenix, 13 Aug 2019. Accessed Sep 2019. www.usenix.org/system/files/soups2019-drury.pdf.
2. 'Know Your Client'. Investopedia, 28 Aug 2019. Accessed Sep 2019. www.investopedia.com/terms/k/knowyourclient.asp.
3. 'EV SSL Certificate Guidelines.' CA/Browser Forum. Accessed Sep 2019. https://cabforum.org/extended-validation/.
4. 'Cyber Actors Exploit 'Secure' Websites in Phishing Campaigns.' Internet Crime Complaint Centre, 10 Jun 2019. Accessed Sep 2019. www.ic3.gov/media/2019/190610.aspx.