

Study Finds 99.99 Percent Probability That Websites with Company-Branded Address Bars Represent a Legitimate, Trusted Domain

Submitted by: Sectigo

Tuesday, 30 July 2019

Georgia Tech Cyber Forensics Innovation Lab Studied 2.6 Million Certificates to Determine Correlation Between Online Crime and Sites with Extended Validation

ROSELAND, N.J. – July 30, 2019 – In 2018, phishing attacks were attempted 482.5 million times (<https://securelist.com/spam-and-phishing-in-2018/89701/>), more than doubling the number of incidents in 2017. New research conducted by the Georgia Institute of Technology Cyber Forensics Innovation (CyFI) Laboratory (<https://cyfi.ece.gatech.edu/>) confirms that a website with a company-branded address bar greatly decreases the chance of internet users falling victim to a malware attack or phishing (fraud) scam. Sponsored by Sectigo (<https://sectigo.com/>), the world's largest commercial Certificate Authority (CA), the CyFI Lab's research concluded that the presence of an Extended Validation (EV) SSL certificate represents a 99.987% likelihood that the site it represents is not associated with common forms of online crime.

The conclusion means that EV certificates play a critical role in assuring consumers that the website they are visiting is legitimate and safe to interact with – playing a much-needed role in online trust.

“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,” explained Dr. Brendan Saltaformaggio (<https://saltaformaggio.ece.gatech.edu/>), Professor & Director of the CyFI Lab, and co-author of the study, Understanding the Role of Extended Validation Certificates in Internet Abuse. “The probability that an EV SSL certificate is associated with a bad domain is less than 0.013%. Our findings reinforce the notion that consumers should view EV certificates as a browser security indicator for trusted domains.”

To conduct the study, researchers at the CyFI Lab cross-correlated a global repository of web domains with EV certificates against an aggregation of web domains associated with malware, suspicious activity blacklists, and underground marketplace communications. CodeGuard, a leader in website backup and recovery and a Sectigo brand, funded the study on a “no strings” basis, ensuring that CyFI was free to design and conduct the study and publish its own independent conclusions.

EV SSL Enables Consumers to Protect Themselves from Online Fraud

SSL certificates (<https://searchsecurity.techtarget.com/definition/digital-certificate>) create a secure communication tunnel by encrypting the data sent between a client and server, or between two servers, to prevent cybercriminals from modifying data. When an active SSL certificate is present, users see a padlock (and never a “Not Secure” warning). There are three types of SSL certificates organizations use on their web pages:

- Good – Domain Validation (DV): The Certificate Authority confirms only that the registered domain is under the control of the certificate requestor. No other identifying information is validated or

provided.

- Better – Organization Validation (OV): The Certificate Authority authenticates not only domain control, but also the identity of the legal entity or individual that requested the certificate. OV certificates provide a higher level of identity validation than DV certificates.
- Best – Extended Validation (EV): The Certificate Authority follows a uniformly high set of authentication procedures (<https://sectigo.com/blog/seven-steps-to-ev-ssl-issuance>) specified by the governing industry standards body to ensure that the true identity of the certificate holder is represented. Popular browsers display the authenticated company name in the address bar, often in the color green. EV represents the highest level of identity authentication an online business can receive.

“The presence of EV influences consumers’ perception of a brand or company,” said Tim Callan, Senior Fellow, Sectigo. “EV certificates are reliably authenticated using techniques that have proven effective through a decade of industry-wide use. EV is a powerful tool to protect consumers from phishing and communicates that an online business has elected to use premium security practices.”

Tips for Staying Secure and Safe Online

According to PhishLabs, more than half of all phishing sites now use SSL certificates (June 2019) (<https://info.phishlabs.com/blog/more-than-half-of-phishing-sites-use-https>). To avoid phishing scams when browsing a website online or opening a link in an email message, Sectigo recommends that consumers look for the full company name at the left of the address bar to ensure the site is really part of the intended online business. In addition, a user should never input credit card numbers, personal information, logins, or other sensitive data on any web page that is not secured with a certificate (as indicated by a padlock in the URL).

About the Georgia Institute of Technology Cyber Forensics (CyFI) Innovation Laboratory

Researchers at the Georgia Tech CyFI Laboratory work together to further the investigation of advanced cyber-crimes and the analysis and prevention of next-generation malware attacks. The lab's work ranges from research in cyber forensics and computer system security to key applications in the vetting of untrusted/malicious software and the protection of critical cyber-infrastructure. To learn more about the CyFI Lab, visit [<https://cyfi.ece.gatech.edu>/<https://cyfi.ece.gatech.edu>].

About CodeGuard and Sectigo

CodeGuard (<https://www.codeguard.com/>), a Sectigo (<https://sectigo.com/>) company, is a global leader in website maintenance, backup and disaster recovery. Sectigo (formerly Comodo CA) provides award-winning (<https://sectigo.com/awards>) purpose-built and automated PKI management solutions to secure websites, connected devices, applications, and digital identities. As the largest commercial Certificate Authority, trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. For more information, visit www.sectigo.com (<https://sectigo.com/>).

Elliot Harrison
Positive Marketing
+44 (0)20 3637 0649
eharrison@positivemarketing.com