BROWSER UI SECURITY INDICATORS

Examples of recent browser UI security indicators

Browser UI security indicators are constantly changing from one version number to the next, and there is little consistency among browsers even for the UI security indicator for any given type of TLS/SSL digital certificate. For this reason, users have a hard time understanding what any particular browser UI means as to user security.

From time to time, the CA Security Council will update this table to show recent browser UI security indicators among the browsers and for unencrypted websites as well as for encrypted websites using different levels of certificates – domain validated (DV), organization validated (OV), and extended validated (EV). CASC would like to encourage browsers to work together and coordinate their UI security indicators, and then stabilize their choices from one browser version to the next, so that users can better understand how to interpret the UI information for enhanced safety.

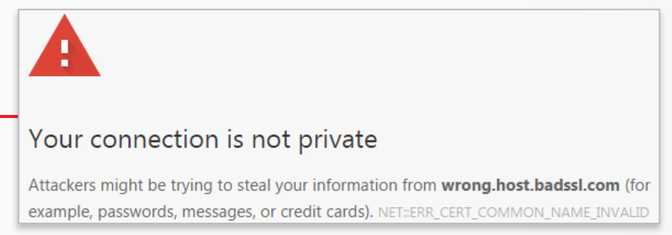
Browser UI Security **INDICATORS** as of December 2016:

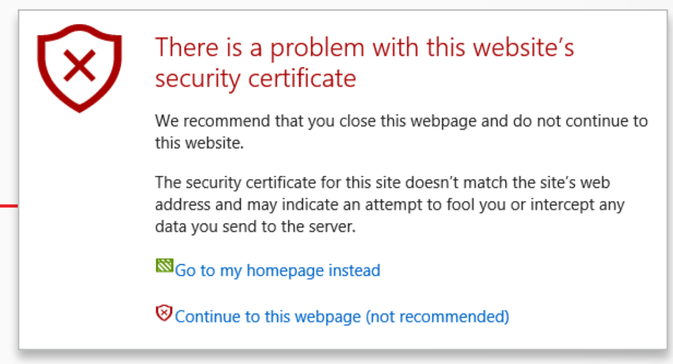
Browser UI Security Indicator:	HTTP only (no certificate)	DV certificate	OV certificate	EV certificate
Chrome 55 (Windows)	www.example.com	https://casecurity.org	https://www.example	Trustwave Holdings, Inc. [US] | https://www.trust
Chrome 48 (Android)	www.example.com	https://casecurity.cor	https://www.example	https://www.entrust.com
Edge 20 (Windows)	example.com	casecurity.org	example.com	https://www.symantec.com
Firefox 50 (Windows)	www.example.com	https://casecurity	https://www.exar	COMODO CA Limited (GB) | https://crt.sh
Safari 9 (Mac)	example.com	casecurity.org	example.com	GMO GlobalSign Inc
Safari 10 (iOS)	example.com	casecurity.org	example.com	DigiCert, Inc.
OperaMini 14 (Android)	www.example.com	casecurity.org	www.example.con	www.godaddy.com
UC Mini 10 (Android)	Example Domain	CA Security Council	Example Domain	https://www.digicert.com
UC Browser 10.8.7.903 (iOS)	example.com	CA Security Council	example.com	SSL & Digital Certificates by GlobalSign

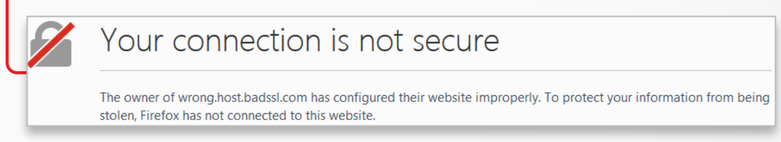
Browser UI Security **WARNINGS** as of December 2016:

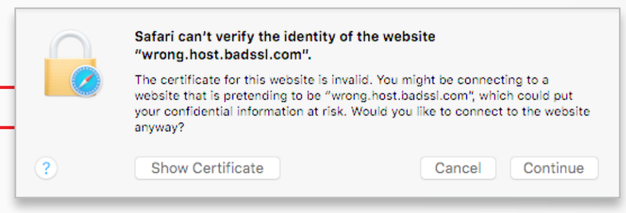
In addition, browsers also provide warnings to users when encrypted (https) pages include minor and major security errors. Here are recent examples of those browser UI security warnings.

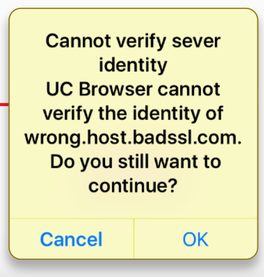
Browser UI Security Indicator:	HTTPS Minor Error	HTTPS Major Error
Chrome 55 (Windows)	https://mixed.badssl.com	~~https~~://wrong.host.badssl.com
Chrome 48 (Android)	https://mixed.badssl.com	~~https~~://wrong.host.badssl.com
Edge 20 (Windows)	mixed.badssl.com	wrong.host.badssl.com
Firefox 50 (Windows)	https://mixed.badssl.com	https://wrong.host.badssl.com
Safari 9 (Mac)	mixed.badssl.com	wrong.host.badssl.com
Safari 10 (iOS)	mixed.badssl.com	wrong.host.badssl.com
OperaMini 14 (Android)	mixed.badssl.com	wrong.host.badssl.com
UC Mini 10 (Android)	mixed.badssl.com	Error!
UC Browser 10.8.7.903 (iOS)	mixed.badssl.com	wrong.host.badssl.com











Click to learn more about UI indicators
https://casecurity.org/identity

CA Security COUNCIL